

# **NATO C3 TECHNICAL ARCHITECTURE**

## **IMPLEMENTATION HANDBOOK (NC3TA-IHB)**

**Version 1**

**Date: 16 December 2002**

**ISSC NATO Open Systems Working Group**



## Table of Contents

0.	EXECUTIVE SUMMARY .....	1
1.	INTRODUCTION .....	3
1.1	NC3TA APPLICABILITY .....	3
1.2	CONTEXT OF THE NC3TA .....	3
1.3	PURPOSE OF THE NC3TA IMPLEMENTATION HANDBOOK (NC3TA-IHB) .....	4
1.4	INTENDED AUDIENCE .....	4
1.5	POINT OF CONTACT FOR THE NC3TA-IHB .....	4
2.	PROGRAM MANAGEMENT .....	7
2.1	INTRODUCTION .....	7
2.2	OPEN SYSTEMS ARCHITECTURAL CONCEPT .....	7
2.3	CONSISTENCY WITH THE NATO INTEROPERABILITY ENVIRONMENT (NIE) .....	8
2.4	DEVELOPING NC3TA-COMPLIANT INFORMATION SYSTEMS .....	9
3.	CONCEPT PHASE .....	13
3.1	INTRODUCTION .....	13
3.2	INTEROPERABILITY REQUIREMENTS .....	13
4.	DEFINITION PHASE .....	15
4.1	INTRODUCTION .....	15
4.2	ARCHITECTURE COMPLIANCE .....	15
4.2.1	Standards Technology Forecast .....	15
4.2.2	Architectural Configurations .....	16
4.2.3	Functional Configurations .....	17
4.3	SECURITY .....	20
4.3.1	PKI Definition .....	21
5.	PROCUREMENT PHASE .....	23
5.1	INTRODUCTION .....	23
5.2	NCSP STANDARDS COMPLIANCE .....	23
5.2.1	Standards Technology Forecast .....	24
5.2.2	Deviation from NCSP .....	24
5.2.3	Technical Configurations .....	24
5.2.4	Internal Interoperability Profiles .....	25
5.2.5	External Interoperability Profiles .....	27
5.2.6	Interoperability Profile Selection/Development Process .....	30
5.2.7	Software Configurations .....	31
5.3	NCOE PRODUCT COMPLIANCE .....	32
5.3.1	Selection from the NCOE Basket of Products (BoP) .....	32
5.3.2	Deviation from BoP .....	33
5.3.3	Integration and Runtime Environment .....	33
5.4	CONFORMANCE, INTEGRATION AND INTEROPERABILITY TESTING .....	35
5.4.1	Introduction .....	35
5.4.2	Interoperability Testing .....	37
5.4.3	Standards Conformance Testing .....	41
5.4.4	Integration Testing .....	43

6.	USAGE PHASE (O&M)	45
6.1	INTRODUCTION	45
7.	SUPPORT	47
7.1	INTRODUCTION	47
7.2	METHODOLOGY	47
7.3	DISSEMINATION OF INFORMATION	47
7.4	TOOLS	47
7.5	TRAINING FOR USING THE NC3TA	48
	ANNEX A NC3TA COMPLIANCE TEMPLATES	49
A.1	C3 INTEROPERABILITY REQUIREMENTS (NSV-11)	51
A.2	FUNCTIONAL CONFIGURATIONS (NSV-12)	59
A.2.1	Introduction	59
A.2.2	Functional Configuration Template	61
A.3	PROJECT STANDARDS PROFILE (NTV-1)	63
A.4	STANDARDS TECHNOLOGY FORECAST (NTV-2)	64
A.5	TECHNICAL CONFIGURATIONS (NTV-3)	65
A.5.1	Introduction	65
A.5.2	Technical Configuration Template	65
A.6	SOFTWARE CONFIGURATIONS (NTV-4)	67
A.6.1	Introduction	67
A.6.2	Software Configuration Template	67
A.7	INTEROPERABILITY PROFILE SELECTION/DEVELOPMENT (NTV-5)	69
A.7.1	Selection of Profiles	69
A.7.2	Definition of Profiles	72
A.7.3	Characterisation of Profiles	73
A.7.4	Example Profile for Certificate Request	74
A.8	NCOE PRODUCT SELECTION REPORT (NTV-6)	75
	ANNEX B EXAMPLE TEST PROCEDURE	77
	ANNEX C NATO AND NATIONAL CM PROCEDURES	81
C.1	BI-SC CM PROCEDURE	81
C.1.1	CIS ORGANISATION AND MANAGEMENT	81
C.1.2	Configuration Management Responsibilities	83
C.1.3	Configuration Management Process	85
C.1.4	Configuration Control Office (CCO) Processes	86
C.1.5	Engineering Change Proposal (ECP) Process	87
C.2	NETHERLANDS CM PROCEDURE FOR LAN2000	90
C.2.1	LAN2000 release management strategy and organisation	90
	ANNEX D NC3TA TOOLS	95
D.1	INTRODUCTION	95
D.1.1	Tool to support the selection or development process of interoperability profiles.	95
	ANNEX E REFERENCES	99

## **0. EXECUTIVE SUMMARY**

In February 2002 the Information Systems Sub-Committee (ISSC), on behalf of the NATO C3 Board (NC3B) approved version 3 of the NC3TA. The NC3TA consists of 5 volumes supplemented by a Rationale Document and this Implementation Handbook. Three of these volumes (Volumes 2, 4 and 5) provide information required to design and implement NATO C3 Systems (NC3S) as directed by NATO C3 policies described in the NATO Policy for C3 Interoperability and NATO C3 Interoperability Management Plan (NIMP) Volume 2.

The North Atlantic Council-approved NATO Policy for C3 Interoperability requires NATO authorities to implement NC3S with the standards and products specified in the NCSP (NC3TA Volume 4) and NCOE (NC3TA Volume 5). In addition, the NC3B approved Architectural Framework contained in NIMP Vol. 2 describes Overarching, Reference and Target Architectures; the Operational, System and Technical Views of architectures; and the templates required to develop these 3 views.

The NATO Open Systems Working Group (NOSWG) recognised the need for an NC3TA Implementation Handbook to provide guidance on how to use the NC3TA in the development and implementation of NC3S in accordance with the above policies. Planners, architects, designers, implementers and maintainers of NC3S will find this handbook useful in performing their respective responsibilities.

This implementation handbook addresses how the NC3TA can be used during the four phases of the NC3S life cycle (i.e. Concept, Definition, Procurement, Usage). Although the major impacts of the NC3TA are on the Procurement and Usage phases, it also has impacts on the Concept and Definition Phases.

During the Concept phase interoperability sub-degrees (described in NC3TA Vol 2) provide a mechanism to help refine interoperability requirements. In the Definition phase NC3TA concepts provide templates for building blocks that are used to develop the Technical View and part of the System View of Reference Architectures. In the Procurement Phase special emphasis is placed on utilisation of NCSP standards and NCOE products in the development of Target Architecture, TBCEs and SOWs. In the Usage phase one requires configuration management of the fielded system baseline architecture, including standards and products.

Since this implementation handbook focuses on the impact of the NC3TA on the development and implementation and NC3S, a companion handbook will be required to address the development of operational and system view templates that are not covered by this handbook. The Interoperability Sub-Committee (ISC) will develop this complementary handbook.

# **1. INTRODUCTION**

## **1.1 NC3TA APPLICABILITY**

The NATO Consultation Command and Control Technical Architecture (NC3TA) is defined as: The minimal set of rules governing the specification, interaction, and interdependence of the parts or elements of NC3 Systems whose purpose is to ensure interoperability by conforming to the technical requirements of all NC3TA Volumes. The NC3TA identifies the services, building blocks, interfaces, standards, profiles and related products and provides the technical guidelines for implementation of NC3 Systems.

The NC3TA supports the bottom-up development of the Technical View and part of the System View for the Overarching, Reference and Target Architectures of NC3S and provides guidance for the appropriate sections of the Capability Package (CP) and Type B Cost Estimate (TBCE). At the Overarching Architecture the focus is on the overall Operational and System View looking at all systems concerned. At the Reference Architecture the focus is more on the detailed Operational and System View of a single system, whereas at the Target Architecture the focus is on the implementation details of both System and Technical Views. The NC3TA provides models and concepts that will aid in the development flow from the more conceptual and logical Operational and System Views towards the more physical Technical View. However, architectural development is an iterative process. The Overarching Architecture aims to tie together the follow-on Reference and Target Architectures. Decisions taken at the Reference Architecture might have to be fed back into the Overarching Architecture whereas technical decisions taken at the Target Architecture will often need to be fed back into the Reference Architecture. The three architectures will need to stay consistent at all times.

## **1.2 CONTEXT OF THE NC3TA**

The NC3TA comprises five volumes that each contribute to the development of the System and Technical Views of NC3S Overarching, Reference and Target Architectures. The NC3TA is supported by a Rationale Document and this Implementation Handbook

Volume 1 of the NC3TA addresses the internal configuration management of all volumes of the NC3TA (maintenance, updating, handling of standards and products, etc).

Volume 2 covers the NC3TA related models and provides information on emerging system architecture related technology. The concepts of Functional Configurations and Interoperability Profiles provide the building blocks to develop the architectural flow from the conceptual and logical System View towards the more physical Technical View. The Sub-degrees of Interoperability allow one to structure the interoperability requirements within the Operational View in order to map them more easily onto standards and products.

Volume 3 is the NC3TA repository of standards information. Standards and detailed profiles are described in terms of their applicability to NATO. It provides direct links to sites where more information on the standards can be obtained.

Volume 4 or the NATO Common Standards Profile (NCSP) contains all mandatory and emerging standards. A separate Rationale Document has been developed to inform the reader on how and why standards have been selected. It should be noted that standards selection draws from the recommendation of responsible committees and working groups wherever appropriate.

Volume 5 or the NATO Common Operating Environment (NCOE) provides information of how computer platform services should be architecturally structured to allow for a smooth evolution. It also includes a “Basket of Products” that comprises the pool of tested and approved products from which projects must select.

The NC3TA Rationale Document defines the process and rationale for selecting services and standards for inclusion in the NCSP (volume 4). It also includes a traceability matrix that tracks the progressive evolution of NCSP standards.

### **1.3 PURPOSE OF THE NC3TA IMPLEMENTATION HANDBOOK (NC3TA-IHB)**

The concepts of the NC3TA require proper implementation guidance. In order to select from the mandatory standards and products and to comply with the broader NATO Interoperability Environment (NIE), the NC3TA-IHB provides implementation guidance for the development of CPs, Type B Cost Estimates (TBCEs) and Technical Views for NC3S Overarching, Reference and Target Architectures. This guidance includes the NC3TA related management processes, interoperability requirements capture, and the overall validation, integration and testing requirements. The implementation aspects of the NC3TA will impact all Life-cycle Phases, and this Handbook will therefore address the relevant aspects at the Concept, Definition, Procurement and Usage Phases.

### **1.4 INTENDED AUDIENCE**

As the NC3TA-IHB impacts on the full NATO Project Life cycle, the user community of the NC3TA-IHB can comprise technical project managers, procurement staff, architects and IT specialists. This includes technical staff from NATO Working Groups that need to select or develop profiles or from O&M Organisations such as NACOSA.

Although the NC3TA-IHB is primarily developed for the implementation and maintenance of NATO C3 Systems, it should also provide equal benefit to national project and procurement staff and their contractors, in order to promote the widest possible opportunities for interoperability.

### **1.5 POINT OF CONTACT FOR THE NC3TA-IHB**

The NC3TA-IHB has been developed by the NATO Open Systems Working Group (NOSWG) of the ISSC AC/322(SC/5), together with its specialist sub-group the NC3TA Implementation AHG (NCI AHG). In addition to the formal Sub Committee approval process, comments from NATO or National project staff are welcome and should be addressed to:

Secretary, ISSC

Information Systems and Technology Branch

NATO Headquarters C3 Staff

B-1140 Brussels, Belgium

Email: [iss@hq.nato.int](mailto:iss@hq.nato.int)

The full NC3TA documentation is available on the Web at: <http://194.7.79.15/>



## **2. PROGRAM MANAGEMENT**

### **2.1 INTRODUCTION**

Within the context of the NC3TA, programmatic measures must be applied in an effective and diligent manner in order to help avoid schedule slippage, cost overruns, as well as recurring resource constraints. The following information identifies some of the unique aspects of the NC3TA (in particular volumes 4 & 5) that should be taken into consideration during the entire system life cycle process:

- The NCOE does not favour the use of any NCSP referenced software programming languages over the other, but if an NCSP programming language is selected, the applicable mandated standard shall be applied. Programmatically, the use of formalised standards based languages for application development purposes should be considered on a case by case basis;
- The NCOE is driven by the open systems paradigm. That is to say that the concept of the NCOE is to promote interoperability among diverse systems. However, the actual platform utilised must be in accordance with the requirements, resources, and feasibility factors that have been identified for a particular NCF program;
- For systems development purposes, the NCOE shall utilise commercial-off-the-shelf (COTS) products wherever possible. On a precautionary note, all other off-the-shelf products (e.g., NOTS, GOTS, etc.) shall be used only when deemed appropriate as a preliminary solution;
- All standards referenced products shall be in full conformance with the NIE (see NIETI).

### **2.2 OPEN SYSTEMS ARCHITECTURAL CONCEPT**

The open systems architectural concept is based primarily on the ability of systems to share information among heterogeneous platforms. It is a concept that capitalises on those specifications and services that can support the effective design, development and implementation of software intensive system components. Within an open system, those products selected and utilised must first comply with the agreed upon architecture to be considered truly 'open.' Furthermore, the functionality desired must adhere to specifications and standards in order to be structurally sound. In the technical sense, various characteristics are inherent to the open systems architecture paradigm. Within the context of this document, three particular characteristics for an open system architecture are described below:

*Interoperability* - refers to the ability of two or more systems that can effectively exchange data without loss of attributes; are in a common format understandable to all systems exchanging the data; and exchange data in a manner in which the data is interpreted the same; and use an agreed common set of profiles to support the exchange of data.

**Portability** – The ability of a subsystem component or part (e.g., a database management system, or operating system) to move from one system to another, and;

**Application Integration** – The effect of configuring the system's software into controllable units via a regimented segmentation process. This includes the ability to provide a seamless user interface that looks, feels, and behaves in a manner that is conducive to the end user and/or developer (i.e., performs the same throughout the entire systems environment).

It is important to note that the concept of interoperability and the open systems paradigm are explored in detail within the NATO C3 Interoperability Environment (NIE) and is inclusive of the operational, system, and technical views.

### 2.3 CONSISTENCY WITH THE NATO INTEROPERABILITY ENVIRONMENT (NIE)

The NATO Interoperability Management Plan (NIMP) Volume 2 has defined an NIE Consistency Process. This process intends to capture and specify the information exchange requirements at the appropriate stages of the NC3 System life cycle. This is facilitated by the use of standardised architectural templates. Figure 2-1 below depicts where in the NC3S life cycle the NIE Consistency Data Sheets will need to be provided.

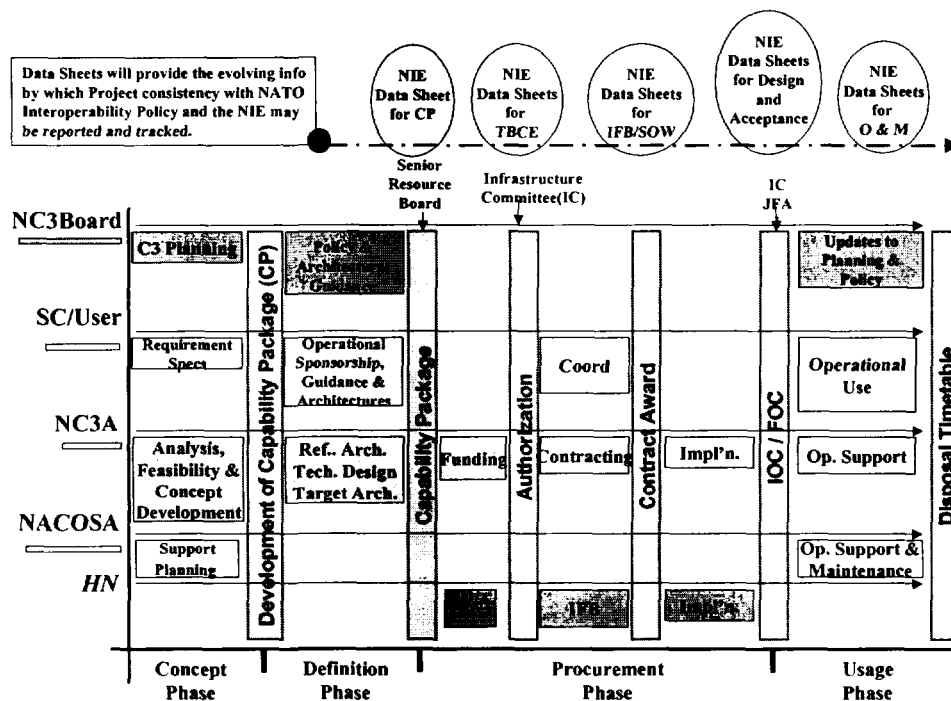


Figure 2-1: NIE Compliance Data Sheet Requirements in the NC3S Life Cycle

In order to maintain a consistent interoperability perspective of a project throughout its life cycle from concept to disposal, the NIMP has introduced a number of NIE Consistency Data Sheets as a modification of and extension to established NATO life cycle management procedures. These Data Sheets are linked directly to critical checkpoints during the C3S life cycle to assess whether NIE consistency has been achieved.

- The initial Data Sheet should be created at the time of Capability Package (CP) development, and will comprise data in the form of Reference Architecture templates. This 'generic' Data Sheet should support, as a composite set, all potential projects contained within the CP;
- Following CP endorsement and as individual TBCEs are derived, their corresponding Data Sheets should be established. These will describe specific architectural templates in more technical detail, and address NCSP standards compliance (and where possible NCOE product compliance);
- As Host Nations proceed through the procurement process of Invitation for Bid (IFB) and contractual award, the individual Data Sheets will contain an increasing level of technical detail, thus providing verifiable evidence of policy and interoperability consistency;
- Ultimately a Data Sheet will form part of the O&M project documentation for the life of the system.

The NIE Consistency Process is described in detail in NIMP Vol 2 chapter 4. The Data Sheets address interoperability consistency for the three architectural views of each system. The NC3TA requires specific templates for the Technical View of each system, which form a subset of templates required within the Data Sheets described above.

## 2.4 DEVELOPING NC3TA-COMPLIANT INFORMATION SYSTEMS

The compliance of NATO CCIS with the NC3TA should be addressed over the whole system lifecycle in order to ensure full consistency of application. In order to support this process it is therefore appropriate to establish a "System/Project Management Life-cycle", as depicted in figure 2-2.

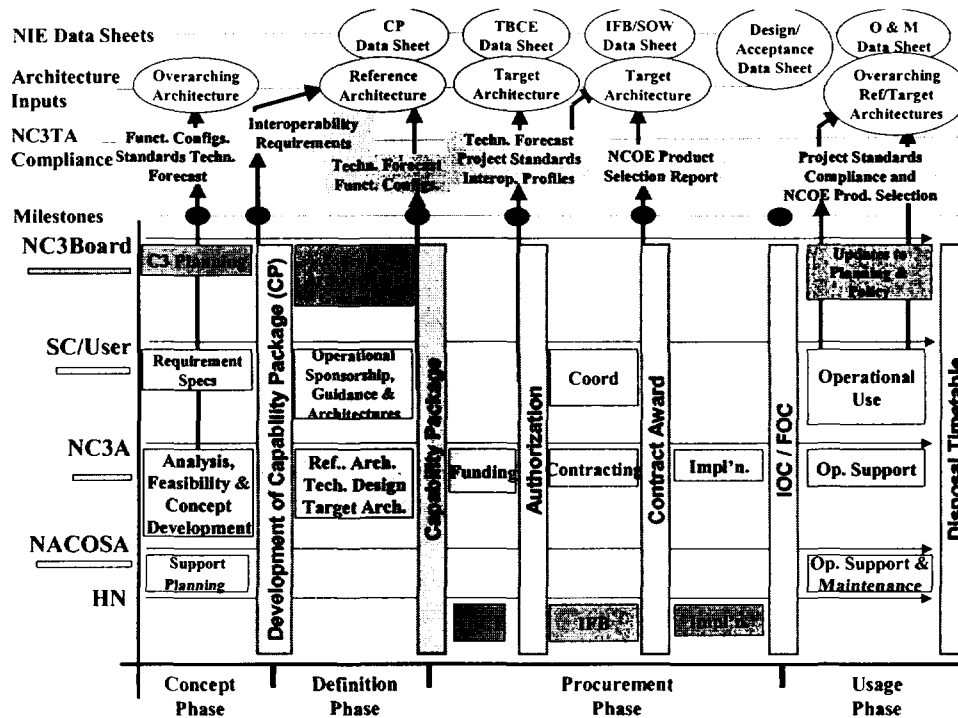


Figure 2-2: NIE and NC3TA related System/Project Management Life-cycle

This Life-cycle links the NC3TA required products with the NIE Data Sheets, and provides guidance as to what inputs should be delivered at which stage.

The Working Group of National Technical Experts on Automated Data Processing (WGNT-ADP), assisted by the NOSWG has the role for influencing System and Project conformance with the standards and products within the NC3TA. Currently, the WGNT-ADP has no assigned role in the procurement phase after TBCE screening. For this purpose NC3TA Compliance Templates have been developed that support the project compliance checking process (see Annex A). These templates each deal with compliance issues in the different life-cycle phases. These templates are proposed for the NIMP Architectural Framework, as NATO System View (NSV) and NATO Technical View (NTV) templates:

- NSV-11: C3 Interoperability Requirements (supporting template) - Annex A.1,
- NSV-12: Functional Configurations (essential template) - Annex A.2,
- NTV-1: Project Standards Profile (essential template) - Annex A.3,
- NTV-2: Standards Technology Forecast (supporting template)– Annex A.4
- NTV-3: Technical Configurations (essential template) - Annex A.5,
- NTV-4: Software Configurations (essential template) – Annex A.6,
- NTV-5: Interoperability Profile Selection/Development (supporting template) – Annex A.7 and,
- NTV-6: NCOE Product Selection Report (essential template) - Annex A.8.

These templates provide architectural guidance and allow requirements versus standards and products tracing and present an overview to Committees of usage of technology, standards and products by projects. In order to contribute to the NIE consistency process, each template is a checkpoint for the different NIE Data Sheets as can be seen in Figure 2.2. To facilitate existing operational requirements and perpetuate interoperability across diverse systems, every standard based product must first adhere to the respective provisions outlined within the NC3TA. This applies to project planning documents (CP and TBCE), as well as to the related architectural documents (Overarching, Reference and Target Architectures).

It is important to note that the Reference Architecture (RA) should be developed in concert with the Capability Package (CP) since the CP can only be approved with an RA attached or the CP containing a project to develop a RA. The NC3TA, most notably volume 2, should be viewed as a point of reference for RA developers in terms of the architectural building blocks (functional configurations), overview of new technology and domain architectures (security, data, directory, etc) that are described therein.

Together with the Type B Cost Estimate (TBCE), the Target Architecture (TA) will need to be developed as well. The TBCE can only be approved with a TA attached. The NC3TA, especially volumes 4 and 5, does provide technical guidance for the TA developer(s) in terms of standards, generic architectural structure and related products.

Figure 2-3 below pictures the relationship of the three types of NC3S Architectures as agreed within NATO. The Overarching Architecture (OA) contains an overview of all related NC3S and their required interoperability. It contains the three Views (Operational, System, Technical), but these are relatively generic. The NC3TA contributes to the OA by providing broad technical guidance in terms of emerging technology, base standards and generic Functional Configurations

(see 4.2.3 and NC3TA Volume 2). The OA emphasises on the interfaces between Functional Configurations and could impact on the NC3TA by identifying new required services or technology that all related systems should adopt. Also domain specific architectures, as referred to in NC3TA Volume 2, could be addressed in the OA in order to make them a mandatory element within all sub-ordinate Reference Architectures. As the OA needs to refer to the NC3TA in broad terms only, further guidance in this handbook concentrates on the development of the System and Technical Views for the Reference and Target Architectures. The OA spans a timeframe of around 10 years and is normally already agreed to form the basis for further development of project specific RAs and TAs. As indicted in the diagram below scope refers to multiple project specific Reference Architectures

The Reference Architecture (RA) is NC3S specific and is also more detailed than the OA. The RA spans a timeframe of about 5 years, although they do not necessarily have to be started at the same starting point. Each RA applies to multiple Target Architectures (TA). TAs are in essence implementation snapshots in time of their related RA, with a time span of 2 years. They are more detailed, especially in the Technical View.

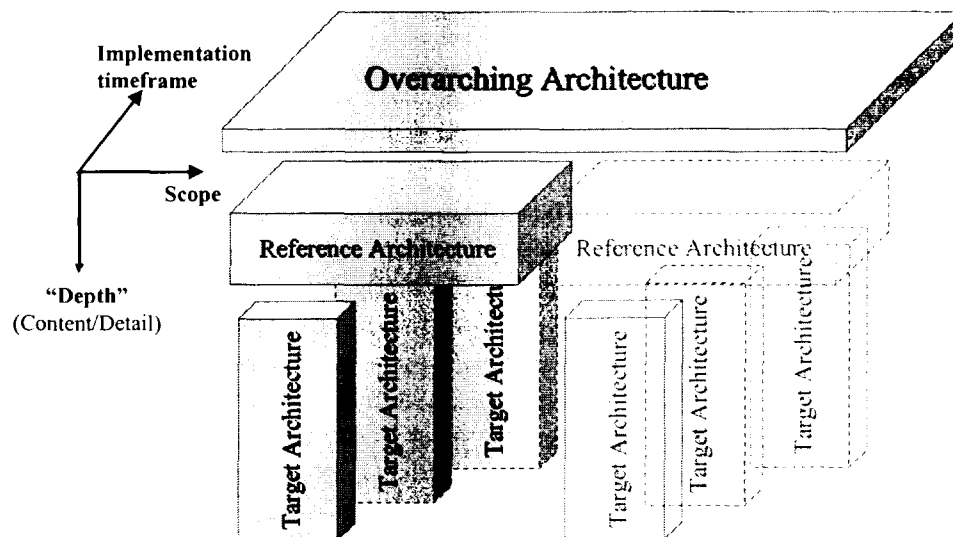


Figure 2-3: Relationship of the three types of Architectures.

The following chapters will address the issues that are of concern for the development of the Project's System and Technical Views for each of the four Life-cycle Phases.

### **3. CONCEPT PHASE**

#### **3.1 INTRODUCTION**

At the Concept Phase the Minimal Military Requirements (MMRs) should be developed as a first step towards the development in the Definition Phase of the Capability Package and related Reference Architecture.

In addition to the MMRs, both Functional and Interoperability Requirements need to be developed in order to get an overview of the sort and the amounts of data that will need to be exchanged accordingly. The requirements should include appropriate information that will allow traceability through further phases. This should be seen as a starting point to monitor the project standardization and subsequently to achieve the NC3TA assigned goals and objectives.

#### **3.2 INTEROPERABILITY REQUIREMENTS**

The starting point for Information Exchange Requirements (IERs) is the data that is captured in the Operational Information Exchange Requirements Matrix (See NIMP Vol II, Architectural Framework section 10-7 and template NOV-4). This Operational View template expresses the relationships in the Operational View across the task, operational elements, and information flow. It identifies the basic elements of the user information in support of a particular activity and between activities.

On the one side these IERs help to capture the information flow between operational units and on the other side help in the dimensioning of the system capacities. Combined they allow the proper selection of the required Interoperability Requirements expressed as Interoperability Sub-degrees (see NC3TA Vol 2). The Interoperability Sub-degrees help refine the interoperability requirements at the appropriate level of detail, as well as enable the definition of the relevant functional interoperability at the Definition Stage. The Sub-degrees of Interoperability in fact form the linkage between the Operational View and System/Technical View, as they allow, together with the Functional Configurations (see 4.2.3 and NC3TA Vol 2), to define the required standards and profiles for the Technical Configurations (see 5.2.2, 5.2.3 and 5.2.4). The Interoperability Requirements should be captured by identifying the required Sub-degrees of Interoperability, using the C3 Interoperability Requirements Template NSV-11 at Annex A.1. This will form the basis for the System View of the Reference Architecture and will be an input to the NIE Data Sheet for the CP stage.

## **4. DEFINITION PHASE**

### **4.1 INTRODUCTION**

In the Definition Phase the project CP and its related Reference Architecture (RA) are being developed. The RA perpetuates an overall global architectural design that is inclusive of the Operational, System and Technical Views. The Definition Phase requires defining and identifying all of the architectural components.

### **4.2 ARCHITECTURE COMPLIANCE**

Both the Technical and (parts of) the System View of the project's RA will need to comply with the NC3TA concepts and standards. This includes the Architectural Configurations, i.e. Functional Configurations (FC) and related functional interfaces for the RA and Technical and Software Configurations for the TA. The RA should also include an overview of the new technology that will impact on the coming Target Architectures.

The RA should in addition adopt the concepts of NATO defined domain architectures where appropriate. Domain architectures include: NATO TACOM Post 2000 Architecture, NATO Security Architecture and NATO Alliance Directory Architecture. These domain architectures each define constraints, but on the other hand solve interoperability issues that would otherwise need to be resolved by each project individually.

The NATO Operational View 3 (NOV-3) and NOV-4 and the C3 Interoperability Requirements (NSV-11) templates developed at the Conceptual Phase will need to be refined into Functional Interfaces, which addresses the communications, data interchange and security protocols and formats between FCs in functional terms.

#### **4.2.1 Standards Technology Forecast**

The RA should provide a Standards Technology Forecast describing the emerging technology standards that might be expected to affect the reference architecture. It contains predictions about the availability of emerging standards and the likely obsolescence of existing standards in specific timeframes (e.g., 5 years for RA and 2 years for TA), and confidence factors for the predictions. It also contains matching predictions for market acceptance of each standard and an overall risk assessment associated with using the standard. The forecast includes potential standards impacts on current architectures, and thus influences the development of target and reference architectures. The forecast should be tailored to focus on technology areas that are related to the purpose for which a given architecture description is being built, and should identify issues that will affect the architecture.

Annex A.4 contains the template NTV-2 addressing the Standards Technology Forecast, required for the System View of the Reference and Target Architectures and will contribute to the NIE Data Sheet for the CP and TBCE stage respectively.

## 4.2.2 Architectural Configurations

Architectural development requires modelling that helps to understand the relationship between requirements on the one side and architectural concepts on the other side. Requirements need to be transformed into architectural “building blocks” that help to more easily portray Overarching, Reference and Target Architectures. In order to smoothen this transformation process, these building blocks need to provide a migration path from functional, to standard/technical and finally to software concepts. The building blocks in these phases are respectively called “Functional Configuration”, “Technical Configuration” and “Software Configuration”.

Functional Configurations (FC) are composed of application and foundation services and interface functionally with one another. Technical Configurations (TC) are assemblies of components and standards that interoperate with other TCs through Interoperability Profiles. Software Configurations (SC) are physical assemblies of products and segments that provide Software Interfaces with other SCs. Figure 4-1 below portrays the ER diagram for the three Architectural Configurations and their relationships.

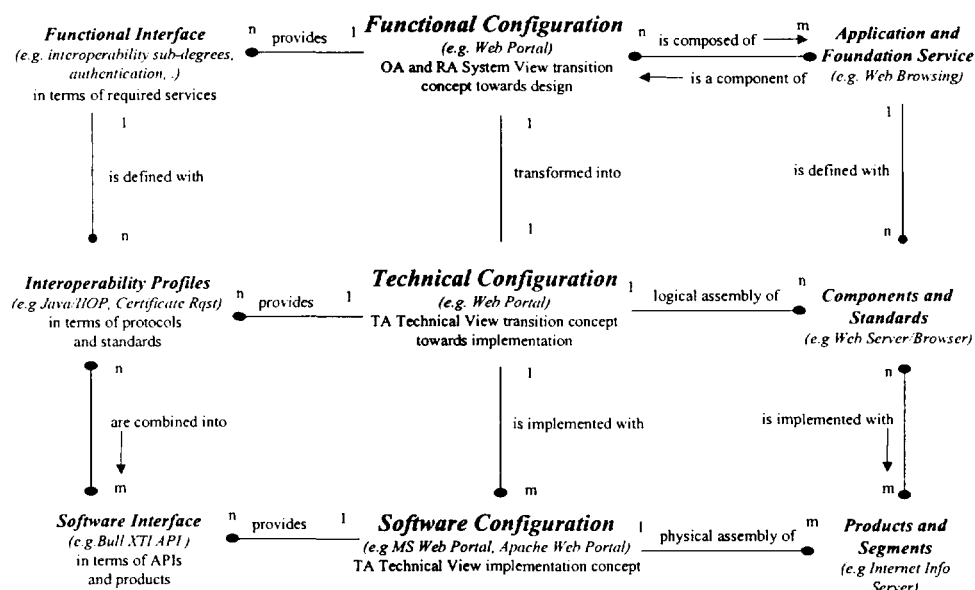


Figure 4-1: Entity Relationship (ER) Diagram for Architectural Configurations

All Configurations in the above figure are models in that they represent a generic template which can be instantiated with different functionality in case of FCs, different technical solutions for TCs and different product solutions for SCs. In fact the diagram at figure 4-1 could be extended to portray Physical Configurations that are an assembly of Software Items, but this would only be relevant to the implementing contractors. In the paragraphs below, each of these concepts is further elaborated.

Paragraph 4.2.3 below addresses the Functional Configurations. Paragraphs 5.2.2 and 5.2.7 address Technical and Software Configurations respectively.



4.2.3 Functional Configurations

Interoperability requirements as documented in NSV-11 templates, are often too coarse to define the necessary standards or profiles for all architectural components. In order to give the user a better understanding of how the requirements are translated into information systems components, the NC3TA has defined the concept of Functional Configurations (FC).

Functional Configurations (FC) are functional building blocks that should be applied during the project’s Concept Phase for the System View description of Overarching Architecture and during the project’s Definition Phase for the System View description of the Reference Architecture at the CP stage. FCs should be seen as a System’s View transition concept towards the design of the Technical View for the Target Architecture, where the related Technical Configurations that include the appropriate components and standards are defined.

An FC consists of a logical assembly of functional components, which collectively can implement a cohesive set of services.

A full overview of FCs is provided in NC3TA Volume 2. In order to minimise architectural complexity it is recommended to reuse as much as possible the FCs defined in volume 2, and refine them into project specific “child” FCs by adding or deleting optional functionality.

An FC may be viewed as the transition vehicle from functional to physical implementation. The graphical depiction of FCs like “user workstation” or “network server” is more meaningful for implementers than a pure listing of constitutive components. The FCs visualise the implementers’ functional viewpoint on the system. See figure 4-2 below for an example FC User Workstation or NC3TA Volume 2 for an overview of all FCs. Annex A.2 contains the NSV-12 template for FCs .

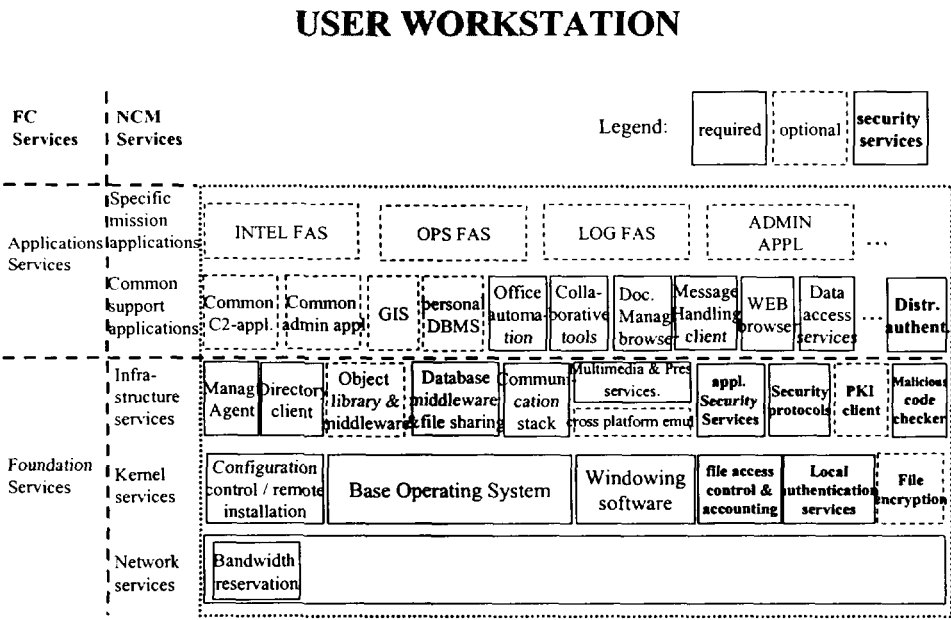


Figure 4-2: Example of an FC User Workstation

A single component may appear in multiple FCs (e.g. the OS and general-purpose components, such as security or management agents...). The same way as the components are product

independent, are the FCs also product independent. However, the system breakdown into FCs is a key architectural decision, which impacts on the final architectural solution. Multiple architectural paradigms, such as thin client/fat client or 2-Tier/3-Tier/N-Tier, may coexist.

FCs functionally interface in terms of required services. In the Procurement Phase, these functional interfaces needs to be translated into elementary or composite interoperability profiles of standards that implement these functional services (see figure 4-1 and paragraphs 5.2.3 and 4).

Eight key FCs, that can be considered as "functional building blocks", have been identified and each can be extended with additional ones if required. The software architectures of these FCs are customisations of the NCOE-component model. They instantiate a subset of the NCOE services and comply with the layered NCM. The components of a defined FC can be viewed as the services of the NCM (for example the "WEB browsing service" is translated into "WEB browser" on the user desktops and "WEB server" on the WEB portal). Figure 4-2 provides on the left both the NCM service layers as well as the more user-oriented application and foundation services.

An example of a system breakdown into key FCs with arrows representing their functional interoperability is given in figure 4-3 below.

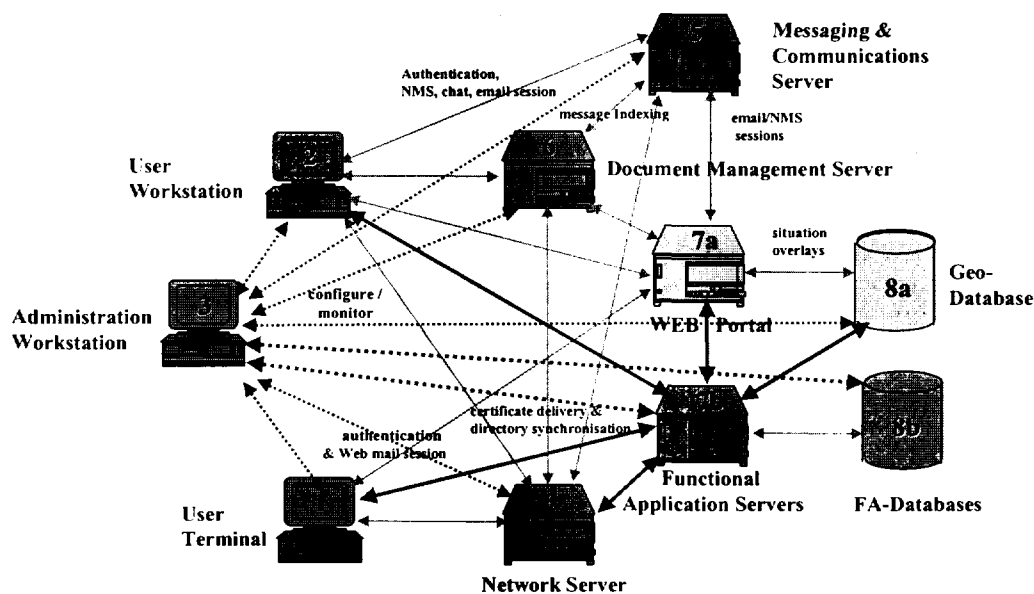


Figure 4-3: Example of Functional Configurations connected through Functional Interfaces

Somewhat like an object-oriented design approach, a defined "parent functional configuration" can be split into "child functional configurations", provided that the parent functional interoperability can also be split between or be re-defined to the child FCs (see figures 4-4 and 4-5). For a defined system the number of FCs selected should remain limited in order to maintain the architectural complexity to an acceptable level. The combination of its FCs and resulting functional interfaces is then called the "System Interoperability Model".

The FCs form a transition concept towards the design phase to become Technical Configurations within the Target Architecture, where they are filled with the standards (see 5.2.2), and eventually implemented as Software Configurations when the products are being selected (see 5.2.7).

The NC3TA volume 2 provides models for FCs that support the development of the Reference Architecture. The FCs as defined in volume 2 are models for both client and server configurations. The use of the NSV-12 Functional Configurations template at Annex A.2 is required for the development of the Technical View and part of the System View of the Reference Architecture and as such for the NIE Data Sheet for the CP stage.

Figure 4-4 below shows the Functional Interfaces between a Web Portal and its connected FCs. The Web Portal FC is split into two child FCs 7a1 and 7a2.

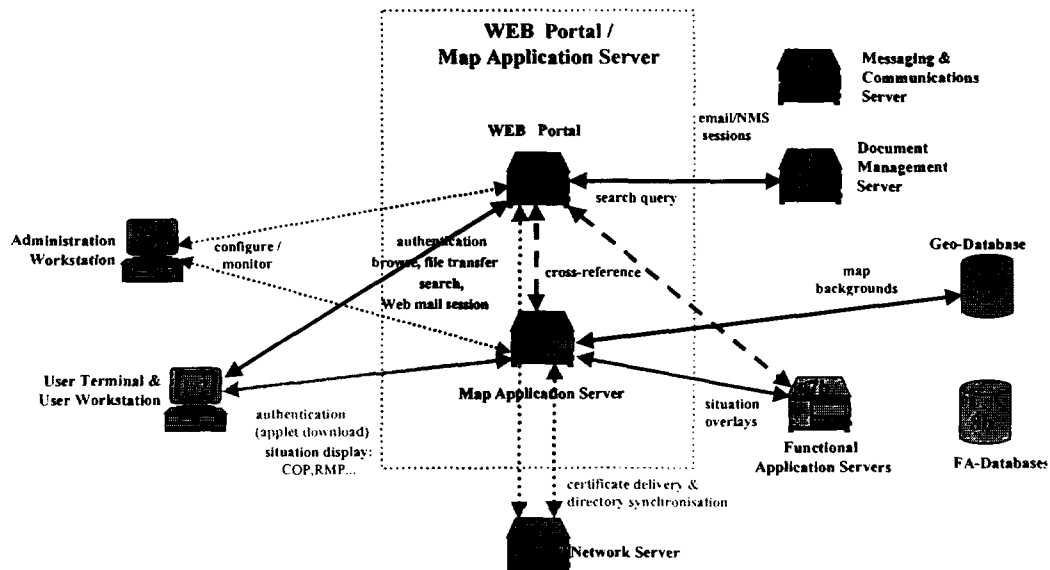


Figure 4-4: Functional Interfaces between a WEB Portal and a Map Application Server.

Many Functional Interface services are available through the products that constitute the computer platform. Important is that products are selected that are based on agreed standards, to improve their interoperability and to allow for easy replacement if required.

The Functional Interfaces in figures 4-4 and 4-5 are for a large part based on standard OTS profiles that are mostly built into products. To allow the technical design of FCs, called Technical Configurations (TC), to better interoperate with each other, it is important to refine in the Procurement Phase the Functional Interfaces of the FCs into the different standards, protocols and their parameters. These are called the Internal or External Interoperability Profiles of TCs (see figure 4-1 and paragraphs 5.2.3 and 5.2.4).

Figure 4-5 below functionally depicts the interfacing with a Messaging FC, which has itself been decomposed into 3 child FCs for Formal Messaging (NMS), Informal Messaging (email) and Instant Messaging (as supported by products such as: ICQ, AIM, or MS-Instant Messenger).

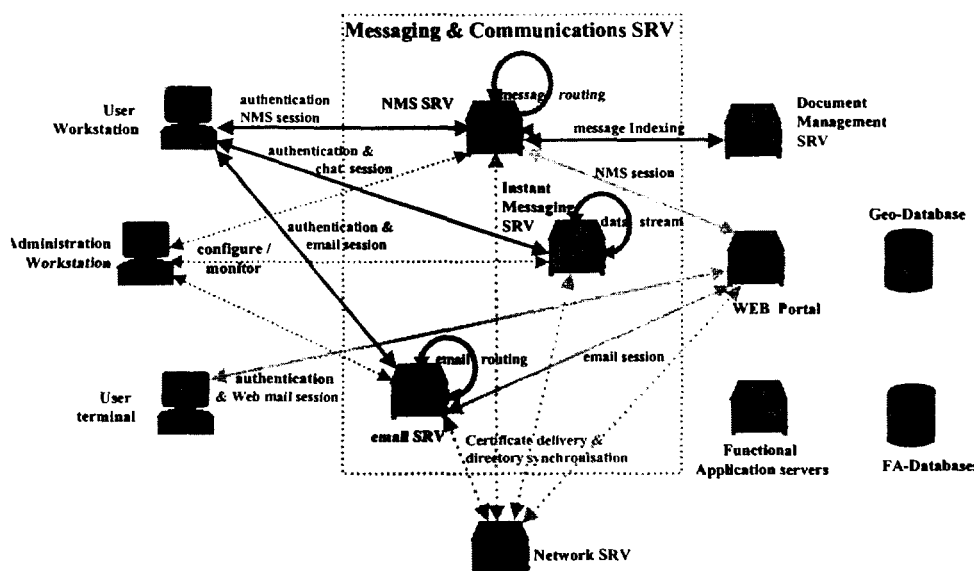


Figure 4-5: Interoperability profiles with a Messaging and Communications Server

### 4.3 SECURITY

Security is a broad concept comprising not only information security, but also personnel, procedures, equipment and infrastructure security measures. In this section we address only the Information Security (INFOSEC), regarding protection of the processed, stored and transmitted information, assuring its integrity, confidentiality, authenticity, accessibility, availability, and non-repudiation. The application of security measures has the objective of achieving a level of trustworthiness with a known and acceptable risk level.

During the Conceptual Phase the required information security services should have been identified through the development of a “Threat and Risk Assessment” document assessing threats and vulnerabilities that have INFOSEC impact (including personnel and physical issues, etc.). It is important to note that the planning of our security mechanisms includes not only the development of the Risk Assessment document, but also the definition of a security policy, operational procedures, contingency plans (disaster recovery, etc.), training, etc. using, where appropriate, Common Criteria terminology and concepts. All the security activities in the life-cycle of communication and Information Systems (CIS), as well as their relationship to INFOSEC directives and guidance are depicted in the document “NATO Security Committee and NC3B Primary Directive on INFOSEC” (ref 8). As stated in this document, all the information in the aforementioned documents should be part of the operational, system and technical views and should form part of the mandatory security annex of the CP.

The services identified during the conceptual phase are to be provided through the mechanisms offered by co-operating authorities/entities hosted in real components identified in functional configurations. In order to identify the profiles required for the interoperation of the security services users with the security services providers, the Definition Phase maps the conceptual security services into a scenario depicting security services providers, security services users and

the supporting communication environment including the networking<sup>1</sup>.

Depending on the user requirements, some or all of these services may be necessary. These services and their distribution within all the Layers of the NCOE Component Model are explained in volume 5 of the NC3TA.

### 4.3.1 PKI Definition

One of the services in volume 5 of the NC3TA within the infrastructure layer is a certificate management service, of which a common example is a public key infrastructure (PKI). A PKI is an infrastructure that allows applications to provide authenticity, confidentiality, integrity and non-repudiation of the information through the assignation of certificates to every entity (users, servers, etc.) so all the information exchanged by these entities is protected from misuse. The PKI offers all the necessary authorities to efficiently manage all these certificates. Figure 4-6 is an example<sup>2</sup> that provides guidance for the drawing of a potential security services scenario.

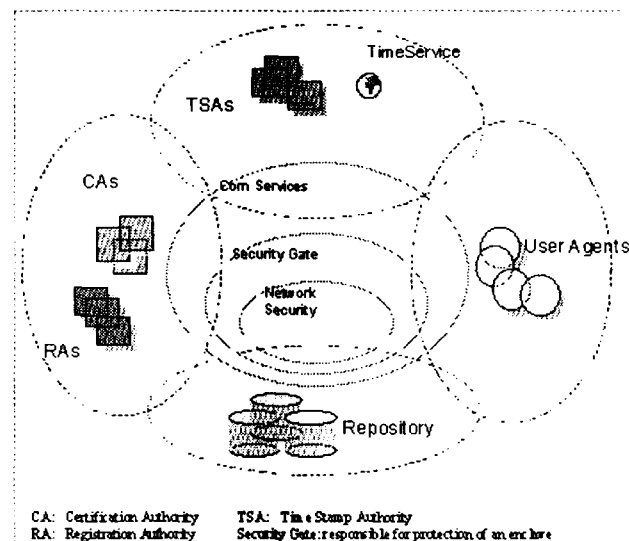


Figure 4-6: Security Policy Scenario

Allocating the security services and adding the points of interactions, the scenario leads to the elementary security functionality required. This security functionality should be combined with the FC functional interoperability.<sup>3</sup>

<sup>1</sup> Some lower level security services may be provided by communication services/network services, such as SSL, IPSec. In some cases the use of these protocols would not be appropriate. For example, the use of IP Sec or SSL to provide a confidentiality service for NATO classified data passing over open networks would not be approved by a NATO security accreditation authority.

<sup>2</sup> Assuming a PKI with rich functionality

<sup>3</sup> For simplification, security services provided by communication services (e.g. messaging) and network layers (e.g. SSL or IPSec) are not shown.

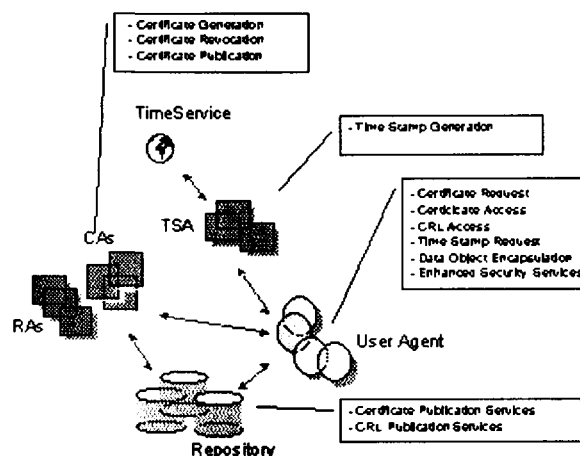


Figure 4-7: Provided Security Services.

Figure 4-7 is used to derive *elementary security functionality* to be combined with the functional interoperability of the FCs.

Examples for derived elementary security profiles are:

- Certificate Request/Response
- Directory Access for Certificates
- Directory Access for Publication of Certificates
- Directory Access for Revocation Lists
- Timestamp Request/Response

Figures 4.6 and 4.7 assume a ubiquitously available NATO PKI with rich services, such as certified time stamping and directory support. There is some risk in a NATO PKI not being implemented in the near term. The NPMA (NATO PKI Management Authority) is an entity under the NC3B meant to develop, among other documents, the NATO policy for the adoption of PKI technology, the CONOPS for the NATO PKI, the corresponding policies (Usage, Certificate, Naming, Recovery and Interoperability Policy), the security Reference Architecture, etc. The NPMA counts with the support of both the PAC (PKI Advisory Cell) and the PKI AHWG (under the INFOSEC Subcommittee (SC/4)), but is somewhat stalled in the development of the NATO PKI. In 2001 the NPMA released the "NATO PKI Implementation Approach, architecture and assignment of responsibilities" (ref 9), which they plan to implement during 2002. Also during 2002 they plan to release the NATO PKI usage and certificate policies, as well as the NATO PKI CONOPS. There is a dependency on the SHAPE CIS/INFOSEC Branch to produce a Bi-SC co-ordinated Capability Package for the pan-NATO PKI.

## **5. PROCUREMENT PHASE**

### **5.1 INTRODUCTION**

As a project moves further along within each phase of the life-cycle process, technical specifications will need to be defined in more detail. Hence, the NC3TA lends itself accordingly, in providing support to the architect and project manager throughout the Procurement Phase.

In the Procurement Phase the Type B Cost Estimate (TBCE) will need to specify the NCSP standards and NCOE products that are considered for the project. The Target Architecture (TA) will define in more detail what standards/profiles and related technology/products will need to be implemented. Volume 4 (NCSP) identifies the mandatory standards in each service area. Volume 3 provides the background information on each standard to allow the selection of appropriate standards for each functional service and in its Annex A contains detailed information on appropriate profiles. The TA should also contain all other standards of concern to the project (e.g. standards not referred to in the NCSP or standards not directly derived from the project interoperability requirement). The NTV-1 Project Standards Profile template at Annex A.3 can serve for this purpose. The standards captured in the NTV-1 template will contribute to the logical description of the Technical View of TAs. The initial profile of standards will form a template for the NIE Data Sheet for the TBCE stage and in a more detailed definitive form for the NIE Data Sheet for the IFB/SOW. The latter should include specific standards profiles that are required for interoperability between NATO Technical Configurations (TC) or NATO and National TCs. These are called Interoperability Profiles.

### **5.2 NCSP STANDARDS COMPLIANCE**

The system/project lifecycle in figure 2-2 shows the NCSP standards compliance required for the TA. Major milestones for NCSP compliance will occur at the following three points in the system development: TBCE stage, IFB stage and Contract Award stage.

Since a considerable period of time (up to 12 months in some circumstances) may elapse following TBCE screening by the WGNT-ADP, through IC fund authorisation, and to issuance of an Invitation for Bid (IFB) by a Host Nation, the NCSP standards and/or NCOE components specified in the TBCE may have been superseded by new standards and/or components. Therefore the HN should specify in the SOW that standards must come from the current version of the NCSP.

The NTV-1 Project Standards Profile at Annex A.3 should serve as a template for this process. It should be used for the development of the Technical View of the TA. Depending on the state of maturity they should initially serve as a template for the NIE Data Sheet for the TBCE and in a later and more mature stage for the NIE Data Sheet for the IFB/SOW.

The NTV-5 Interoperability Profile Selection/Development at Annex A.7 should serve as a template for selecting or developing the detailed Interoperability Profiles between Technical Configurations (see 5.2.2 below).

### **5.2.1 Standards Technology Forecast**

The Target Architecture should include a Standards Technology Forecast describing the emerging technology standards by which it might be affected (see also NC3TA volume 2).

This forecast of the TA should be derived by updating the Standards Technology Forecast of the Reference Architecture with a focus on technology standards affecting more specifically the issues of the TA over a 2 year timeframe.

The template associated to the description of the TA Standards Technology Forecast is identical to the one of the RA, and described in Annex A.4 as NTV-2.

### **5.2.2 Deviation from NCSP**

If a Host Nation (HN) specifies in the SOW a specific standard that is not in the NCSP, the Signals Section of NATO/SILCEP and the NOSWG must be informed. The HN should provide rationale for specifying NCSP relevant standards that are not in the NCSP, and provide plans if they intend to submit such standards for inclusion in future versions of the NCSP. The corresponding fields in the NTV-1 template should be filled in.

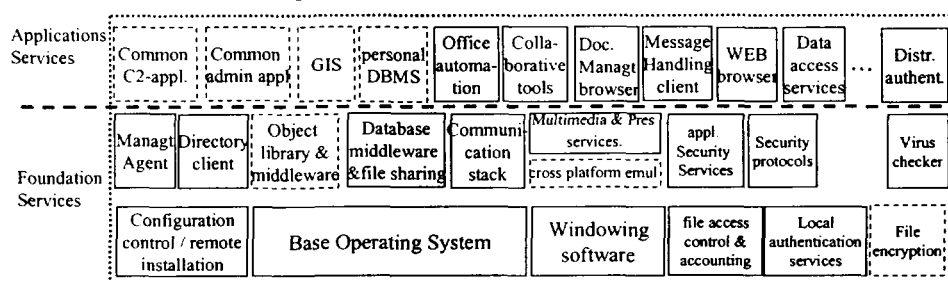
The NOSWG will review the HN request for a waiver for use of a standard not in the NCSP. The NOSWG will provide its recommendation to NATO SILCEP within 6 weeks of receiving the rationale from the HN. If the NOSWG recommends to not grant a waiver for use of a standard that is not in the NCSP, it will provide a rationale supporting its recommendation.

### **5.2.3 Technical Configurations**

Technical Configurations (TC) are a one-to-one technical transformation from FCs. This means that application services as portrayed in FCs are being transformed into components with their respective underlying standards as can be seen in figure 5-1 below. TCs should be seen as a Technical View transition concept towards Software Configurations that define the specific segments and their constituent software products. As there is a one-to-one relationship between FCs and TCs, they have the same name/title (see example under FC and TC in figure 5-1 below).



## FC: USER WORKSTATION



## TC: USER WORKSTATION

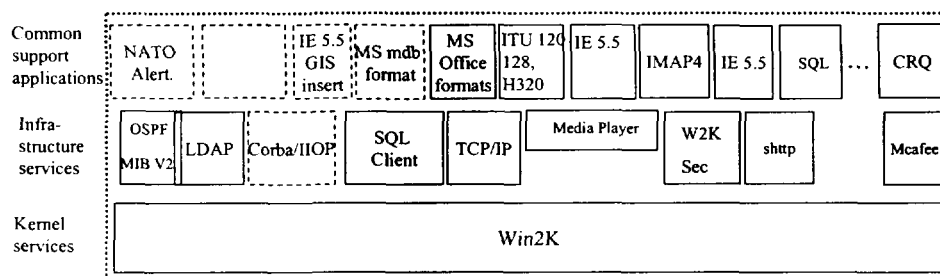


Figure 5-1: Example of User Workstation Functional vs Technical Configuration.

Between TCs Internal Interoperability Profiles (IIP) in terms of protocols and standards will need to be defined. IIPs will normally be embedded within products, and it can therefore not always be avoided that the standards and protocols are proprietary. To allow the flexibility to easily replace obsolete products by new ones, it is recommended to define, where possible, open standards and select products that implement these standards.

### 5.2.4 Internal Interoperability Profiles

An interoperability profile is the interface between two TCs and can be defined as a structured assembly of one or more FC interfaces and associated standards/OTS profiles intended to implement specific interoperability requirements. It may be composed of one or more standard profiles and/or OTS profiles.<sup>4</sup>

If one considers two TCs of the same system, the profile is internal, whereas if the two TCs belong to two distinct systems, the profile is external (see 5.2.4). Two TCs of the same kind and the same system may of course interoperate with each other (e.g. data replication between 2 databases, or message routing between two messaging servers).

Figure 5-2 below shows the different IIPs between TCs. E.g., the IIP between a User Workstation and a Messaging Server (IIP2-5) will define the messaging standards and

<sup>4</sup> A standard profile is a set of one or more base *standards* (listed in the NCSP) providing *services* and *protocols*, including *parameters* and *options*, to accomplish one or more particular *sub-degree(s) of interoperability*.

An *OTS profile* provides "off-the-shelf" communication and/or data processing services that can be tailored with a *set of options and parameters* to accomplish one or more particular *sub-degree(s) of interoperability*.

protocols appropriate for client/server messaging, whereas the IIP between Messaging Servers (shown with the circular arrow IIP5-5) will define the messaging server-to-server protocols and standards.

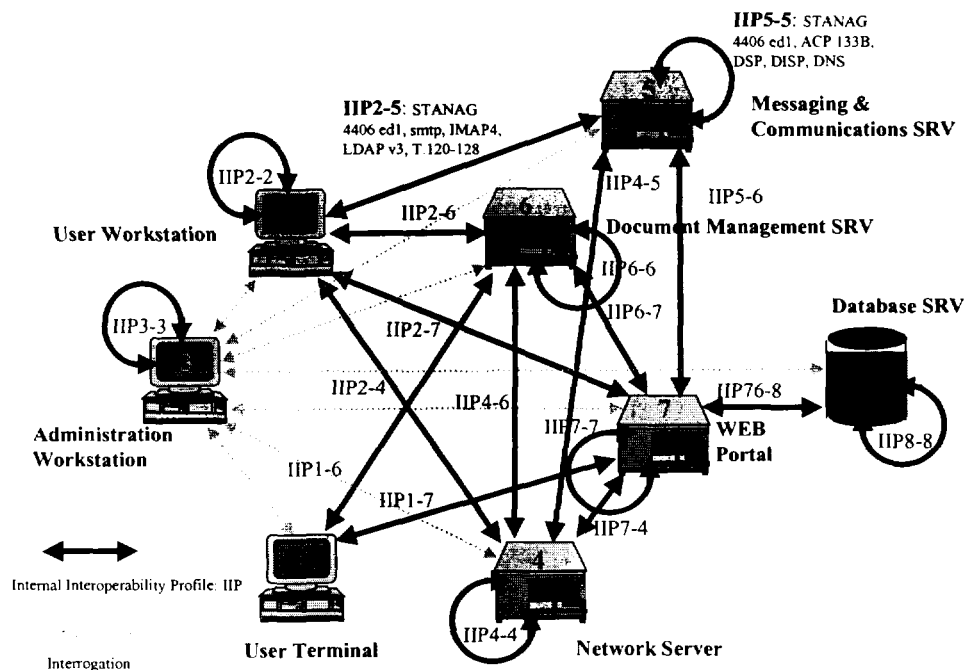


Figure 5-2: FCs with Internal Interoperability Profiles (IIP)

Interoperability profiles are generally speaking “composite” in so far as they support many services and can therefore often be broken down into “elementary interoperability profiles”. Composite and elementary profiles are functionally described in the Definition Phase. At the Procurement Phase the more technical description, including the selection of standards and their more detailed profiles, is addressed.

Many Internal Interoperability Profiles (IIP) are available through the products that constitute the computer platform. Important is that products are selected that are based on agreed standards, to improve their interoperability and to allow for easy replacement if required.

### 5.2.5 External Interoperability Profiles

NC3S will also need to interoperate with other NC3S or National Systems. Therefore guidelines are required to develop External Interoperability Profiles (EIP) that form the interface between different NATO Systems or between NATO and National Systems.

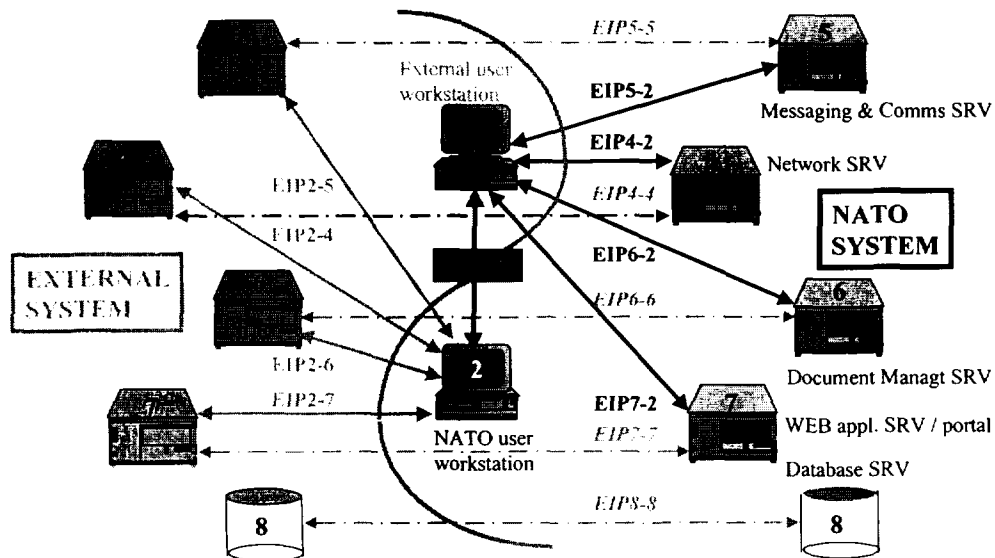


Figure 5-3: External Interoperability Profiles (EIP)

The majority of EIPs from figure 5-3 are standard OTS profiles that are mostly built into products. However, products may differ between national and NATO systems. It is therefore important to agree on the protocols, parameters and data formats that support these EIPs in order to achieve interoperability.

#### 5.2.5.1 NATO with External Systems

Taking the current NATO environment into account, which includes:

- Microsoft Windows 2000 external interoperability aspects (NATO/National Systems),
- Current interoperability trials (e.g. NC3A, COAST, JWID, ICOP, GIS Trial, A-NAUG)<sup>5</sup>,

<sup>5</sup> COAST: Cronos Operational Assessment of Security Technology

JWID: Joint Warrior Interoperability Demonstration

ICOP: Initial Common Operational Picture

A-NAUG: ACE-National User Group

- Security (Message Security Demonstrator Program),

this guidance concentrates on three essential Service Areas: Data Interchange, Communications, and Security. This will offer a structured set of interoperability profiles that may be selected to cover the interoperability requirements of a NATO W2K domain with other NATO or Nations' domains. Other NATO or National domains may be based on W2K, Windows NT, UNIX or Linux operating systems.

#### 5.2.5.2 W2K External Interoperability Boundary

One of the primary goals of W2K is to cover IT requirements of whole enterprises in a single homogeneous environment. Interoperability within that domain is inherent and does not require any profiling, whether in the transport area, communication area, or in the application area. However, this is not true for the external interoperability and security. One cannot assume that the interacting peer domain is based on W2K, and in addition, (according to NC3A evaluations and explorations) W2K Active Directory is applicable and feasible for limited enterprise dimensions only. Therefore, the identification and definition of Interoperability profiles for W2K/Windows NT, W2K/UNIX, W2K/Linux and W2K/W2K interoperability is required.

System complexity on the one hand and robustness and security on the other hand are conflicting goals. From a W2K perspective, this leads even within NATO to a structuring of independent interacting domains, using interoperability profiles. The Microsoft Active Directory (AD) forms an interoperable W2K domain, sub-structured into organisational units or sub-domains. A proposed key concept for NATO to have the W2K AD interoperate with national domains, is the grouping of AD domains and using a *Meta-Directory system* as an interface with national domains, as depicted in figure 5-4.

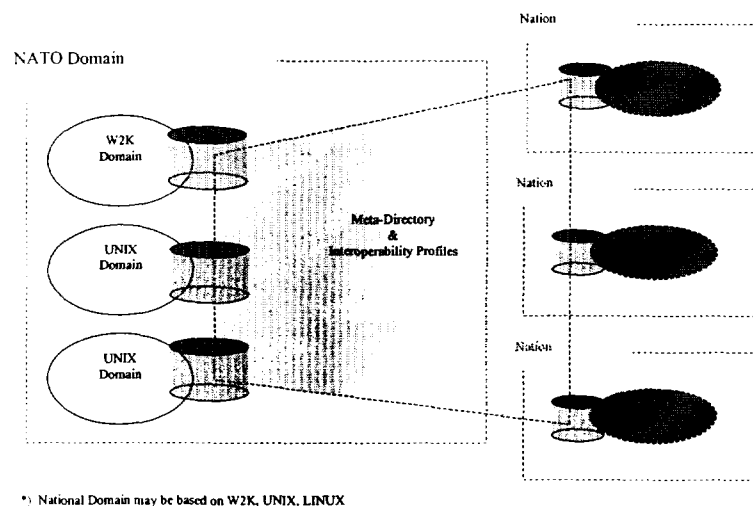


Figure 5-4: NATO W2K Directory Domain

According to the NCOE Component Model, the Meta-Directory should be regarded as an Infrastructure Service. The Directory Schema and appropriate access protocols (LDAP, ACP 133) are critical to external interoperability. In addition, other interoperability profiles are required to cover Data Interchange, Communication and Security Services. For instance

messaging, web access, PKI interactions, authentication services and in particular secure data interchange.

W2K supports authentication services within the same Forest based on Kerberos v5. Authentication among other domains is reached by adopting a concept of trust between these domains. Assuming that a Nation's domain is not based on W2K, the inclusion of authentication mechanisms between NATO and Nation's domains is important. These mechanisms will likely be based on certificates and cross certification.

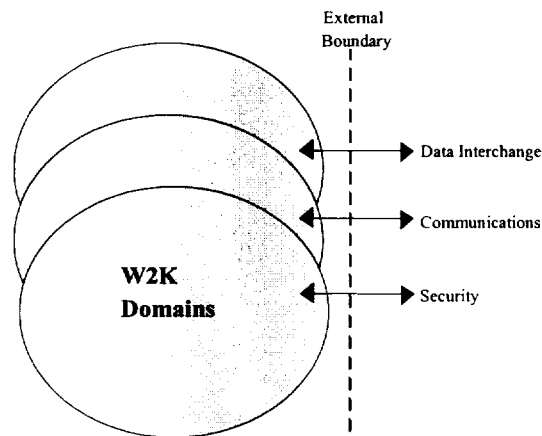


Figure 5-5: Interoperability Boundary NATO/Nations, and NATO/NATO

Data Interchange is concerned with the structuring of data to be exchanged via the external boundaries of a domain using Communication Services. For protection, the data objects transferred may be encapsulated by using appropriate Security Mechanisms.

Based on user interoperability requirements as documented in the NATO Rolling Interoperability Programme (RIP), the following external interoperability profiles are considered:

#### ***Data Interchange***

- Graphic Files
- Audio/Video
- Tactical Digital Data
- Tactical Message Data (AdatP-3, html, MS-Office, pdf, rtf, ...)
- Technical/Business Data (html, xml, MS-Office, pdf, rtf, ...)

#### ***Communication***

- Messaging (STANAG 4406, SMTP, POP3)
- Directory (ACP 133)
- File Transfer (ftp)
- Hypertext Transfer Protocols (http)
- Naming (DNS)

In the profile selection process Directory and Naming profiles are grouped into Infrastructure Profiles, whereas other Communication profiles are regarded as sub-profiles of one specific application and are included as communication service within that particular Application profile.

### ***Security***

- for Data Interchange (Data Object Encapsulation – Cryptographic Message Syntax (CMS))
- for Communication (S/MIME, SSL)
- for Networking (IPSec)
- Key Distribution (Certificate and Revocation List Profiles, PKI Management Protocols, Certificate Request Formats)
- Algorithms (DSA, SHA1)
- Encapsulation Syntax (S/MIME, MIME)
- Directory Schema for PKI-Repository

The list of security base standards provided in the NCSP requires some additional profiles. Annex A.7 Interoperability Profile Selection lists the appropriate profiles. Details on these profiles can be found in NC3TA Volume 3 Annex A.

#### **5.2.6 Interoperability Profile Selection/Development Process**

Before a process for selection or development of interoperability profiles can be performed, the definition of an Interoperability Model which defines all the systems' FCs and their functional interfaces, is required. This is normally done in the Definition Phase as part of the Reference Architecture. With an agreed Project Interoperability Model, which can consist of many smaller profile scenarios, the project staff will be in a position to develop the related TCs and to identify and select existing IIPs and EIPs, or to initiate the development and definition of new profiles, using the process in figure 5-6 and the template NTV-5 at Annex A.7: Interoperability Profile Selection/Development.

During each individual step, a number of tables and examples are available and accessible through a tool to support the process (see 7.4.4). The basis for the development of a new profile is the structure of profiles derived from NC3TA Vol 3 and the guidance for Interoperability Profiles defined in Annex A.7.

It is recommended to go through the proposed Selection/Development Process in figure 5-6 step-by-step and to use the notations proposed in Annex A.7.

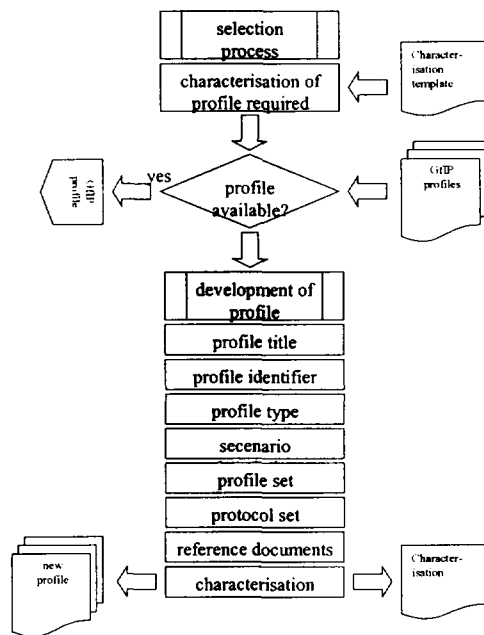


Figure 5-6: Profile Selection/Development Process

### 5.2.7 Software Configurations

Software Configurations (SC) are the software implementation of the related TCs. In principle one would expect a one-to-one relationship between TCs and SCs, but the choice of software products can dictate the actual configuration. Depending on the products, TC-servers might be split into different tiers, or be combined for performance reasons. The SCs are constituted of the actual products that are being implemented, but they are still a model in that they portray the TC's software solution.

As SCs are the software implementation of the related TCs, this means that components and standards, as portrayed in TCs, are being transformed into products and segments as can be seen in figure 5-7 below.

## SC: USER WORKSTATION

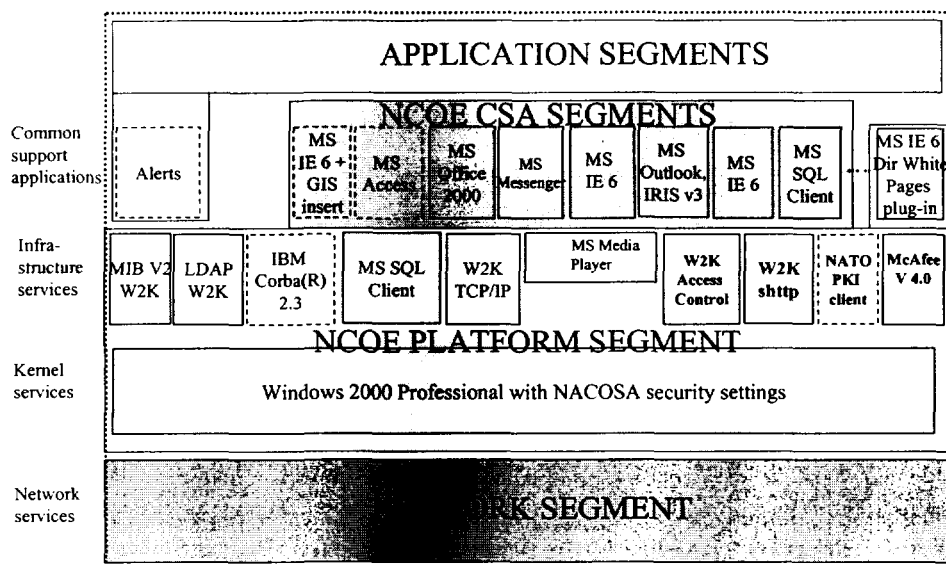


Figure 5-7: Example of Segmented Software Configuration for a User Workstation

Within an NCOE-based SC, the software will be packaged into self-contained units known as segments. Segments are similar to modules of functionality and can easily be added to any supported hardware platform. Segmentation provides the user with the ability to pick and chose from packaged and tested software components deemed necessary for a particular mission. The full segmentation process is described in NC3TA volume 5.

### 5.3 NCOE PRODUCT COMPLIANCE

#### 5.3.1 Selection from the NCOE Basket of Products (BoP)

The NCOE Basket of Products (BoP) in NC3TA Volume 5 contains software products and their constitutive segments that have successfully met the BoP selection criteria described in Volume 5. Included in the selection criteria are: conformance testing with relevant NCSP standards, and integration and interoperability testing. A developer of a NATO C3 System core will have to select from the BoP the suite of products and their constitutive segments necessary for any particular implementation. The design in the Target Architecture must allow for making an estimate on the funding required for the project and should not be considered the ultimate design that will actually be implemented unchanged.

The system/project lifecycle shown in figure 2-2 for NCSP compliance is also valid for NCOE compliance. Major milestones for NCOE compliance in the system development will occur at IFB stage and Contract Award stage. Since a considerable period of time (up to 12 months in some circumstances) may elapse following TBCE screening by the WGNT-ADP, through IC fund authorisation, to issuance of an Invitation for Bid (IFB) by a Host Nation, it is very likely that some of the products, or versions of products in the BoP will have changed.



The NTV-6 NCOE Product Selection Report at Annex A.8 offers guidance in the selection of BoP products. It should be used in the physical descriptions of the Target Architecture, and serve as a template for the NIE Data Sheet for the IFB/SOW.

### **5.3.2 Deviation from BoP**

If a HN specifies in the SOW a product that is not in the BoP, the Signals Section of SILCEP and NOSWG must be informed. The HN should provide rationale for specifying NCOE relevant products that are not in the BoP, and provide plans if they intend to submit such products for inclusion in future versions of the BoP. NC3TA Volume 5 offers a product selection procedure that allows the objective selection and testing of products for inclusion in the BoP. The NTV-6 NCOE Product Selection Report at Annex A.8 will need to be filled in, even if products are not in the BoP.

The rationale for not using components in the BoP could be based on such factors as costs, training, migration constraints and legacy issues. The NOSWG will review the HN request for a waiver for use of a component not in the BoP. The NOSWG will provide its recommendation to NATO SILCEP within 6 weeks of receiving the rationale from the HN. If the NOSWG recommends to not grant a waiver for use of a product that is not in the BoP, it will provide a rationale supporting its recommendation.

The NCOE BoP is comprised of the software products available for NCOE compliant systems and adheres to the standards identified within the NCSP. The software products selected for the NCOE are not limited to a particular hardware platform, and thus platform independent. However, the NCOE Kernel is composed of those components required to be present on all NCOE application platforms.

### **5.3.3 Integration and Runtime Environment**

#### **5.3.3.1 Introduction**

This section describes some of the technical and programmatic requirements necessary for attaining interoperability among NC3S. In addition, it identifies and underscores some of the technical measures necessary for integrating and implementing software components into baseline NCOE compliant systems. NCOE integration and implementation measures are aligned in accordance with the following objectives:

- *Standardization* – Standard adherence is key to interoperability. Used in conjunction with concise development guidelines and training procedures, uniform software components may be built according to program objectives during every phase of the life-cycle process;
- *Portability* – As a rule of thumb, portability promotes vendor independence through the use of commercial-off-the-shelf (COTS) products and de-facto industry standards;
- *Interoperability* – Perpetuate interoperability among NATO common funded systems, as well as National systems. All efforts shall be based on the

interoperability profiling procedures as indicated in Interoperability Profiles Selection/Development Process (see 5.2.6);

- *Scalability* – Systems scalability will be attainable utilising minimal resources wherever applicable. All segments shall be based on the NCOE segmentation concepts in accordance with segmentation procedures in 5.3.3.3;
- *Training* - Maintain a common look and feel in accordance with relevant human computer interface guidelines, configuration management directives and systems administrative operating procedures (regardless of functional domain area);
- *Testing* – Ensure that all standards are accredited and software segments are validated in accordance with NIETI procedures for compliance purposes;
- *Reusability* – The NC3TA defines the core software services and products necessary to promulgate reusability across diverse systems and heterogeneous platform configurations as deemed necessary;
- *Security* - Provide the minimal security measures necessary to protect the system services and user communities from unauthorised access. To provide sufficient measures to protect data from deliberate attack and/or malicious intent.

The NCOE provides the foundation to support the implementation of the core of NATO common and partially funded C3 Systems. The NCOE services are provided in installable software components called segments (see NC3TA Volume 5 for definition of segments). In an ideal world there would be only one segment to provide a specific NCOE function. However, the reality of the NATO procurement policy, the marketplace and the varying needs of system implementers result in multiple NCOE segments with at least some degree of overlap or subset of functionality. System implementers may have to choose between competing segments in the NCOE Basket of Products to achieve their goals for system implementation (e.g. reliability, performance, reduced costs, training, and software compatibility with legacy system).

### **5.3.3.2 Component Considerations**

Selecting software for inclusion within the NCOE is not arbitrary, but is driven by a number of architectural principles and considerations. First of all, a determination must be made on whether or not a particular function is desirable for the NCOE, and then the criteria must be met when selecting the actual component that performs the function desired. A particular function may be determined for the NCOE when it meets the following requirements:

- The function is a part of the software necessary to establish the actual operating environment. Normally, this functionality is provided by COTS products and is inclusive of the operating system, system administrative security features, networking and windowing software;
- The function is necessary in order for data to flow throughout the system. Systems should have the inherent capability to communicate externally with other systems. To do so requires that a system has the capability to manage its own data flow through standardised techniques;
- The function is required for interoperability. Standards by themselves do not ensure interoperability, however utilising common software, common functions and common data storage and interchange components to manipulate common data comes much closer to attaining this objective.

The functions listed above are technical in nature from an architectural perspective and indicate what software must be contained within the NCOE. However, in order to justify the technical functions necessary to adhere to the NCOE, the following points should be taken into consideration from a programmatic point of view:

- The cost of modifying existing code to remove or eradicate duplication across a given system versus the cost of maintaining duplicative code;
- The cost of requiring additional hardware resources necessary for duplicative code/components, and the cost associated with training operators to perform the same type of action(s).
- The NCOE requires that all components are carefully managed and are only changed in a well co-ordinated and controlled manner. This is due to the fact that the NCOE must remain stable and consistent for the objective systems overall integrity.

So any modifications must be done in a succinct, careful and deliberate way. However, changes to the NCOE routines will eventually be customised (if deemed necessary) since it is the objective of an open system based architecture to allow customisation if desired. NCOE components must always adhere to and comply with segmentation principles, procedures, and practices.

#### **5.3.3.3 Segmentation**

Segmentation is an integral feature and important facet of the NC3TA, and can be defined in terms of the functionality that is seen from an end-user's perspective. The segmentation process essentially allows the user(s) to easily add only those required modules that are deemed necessary by the end-user community, thus acting as the building blocks in which open systems can be built. Each building block is known as a segment. Segments are considered compliant in accordance to the degree in which they conform to the specific standards and guidance required for the NCOE. In order to ensure compliance conformity amongst all NCOE segments, it will be necessary to adhere to the rudimentary segmentation compliance process principles defined within Volume 5 and adjoining annexes of the NC3TA.

#### **5.3.3.4 NCOE Kernel Compliance Objectives**

As previously discussed, the NCOE is based on an architectural paradigm that promotes heterogeneity, and thus is not tied to a specific type of hardware platform. However, it should be noted that practicality dictates that the number of platforms supported are limited by the amount of resources readily available. The NCOE focuses on the adoption and utilisation of industry standards, products and services whenever and wherever feasibly possible. These standards, products and services are identified, although not exclusively, within Volumes 4 and 5 of the NC3TA.

### **5.4 CONFORMANCE, INTEGRATION AND INTEROPERABILITY TESTING**

#### **5.4.1 Introduction**

The NIETI CONOPS (ref 2) states that “Conformance and Interoperability testing of the NIE standards and products are vital, to ensure that current and future systems or system components implementing them may interoperate more effectively under a variety of conditions”. In addition to conformance and interoperability testing, integration testing is required to ensure that new software can be installed/uninstalled quickly and correctly. Although all three types of testing are important, interoperability testing is given the highest priority. Interoperability testing is deemed the most important because the Defense Capabilities Initiative<sup>6</sup> primarily focuses on improving interoperability among Alliance forces. Interoperability testing can be used to help assure interoperability of Alliance forces when they are deployed in combined and joint operations.

Since NATO and National C3 Systems are being implemented with an ever-increasing amount of COTS products, NATO will try to make maximum use of brands from commercial organisations dealing with conformance and integration testing (e.g. Open Group and VeriTest). The NIETI team maintains capabilities of commercial testing organisations and a database of compliant commercial products.

The NIETI team has defined 4 types of testing as shown in Figure 5-8.

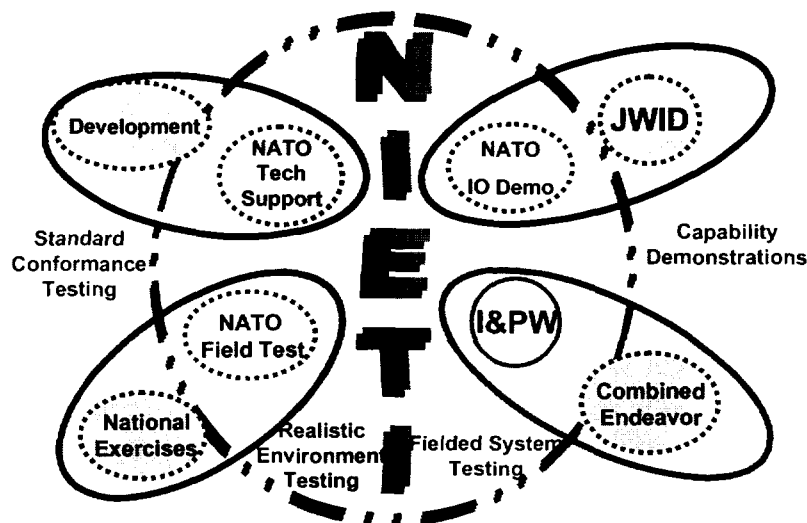


Figure 5-8: NIETI System Interoperability Testing

<sup>6</sup> See item 4 of the Defense Capabilities Initiative issued during the Washington summit 23-24 April 1999.

For NC3TA related testing this figure has been slightly modified as shown in Figure 5-9. The change was to add NCOE integration testing to complement interoperability (pre-deployment and fielded system) and standard conformance testing.

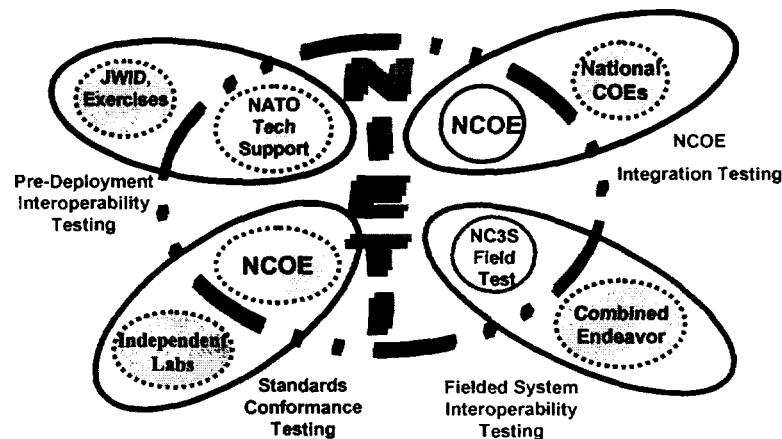


Figure 5-9: NC3TA Related Testing

#### **5.4.2 Interoperability Testing**

Fielded System Interoperability Testing (e.g. Combined Endeavor) and Pre-Deployment Interoperability Testing (e.g. JWID) involve systems from multiple nations and agencies. Since many organisations are involved in this type of interoperability testing, one is not able to concentrate on detailed interoperability testing between any two specific systems. Therefore additional types of interoperability testing are required between NATO to NATO systems and NATO to National systems. Additional information on Combined Endeavor may be found at <http://www.pcc.pims.org/Projects/CE/index.htm>. More information on JWID may be found at <http://www.jwid.js.mil>

Two key points concerning interoperability are that compliance to standards does not guarantee interoperability and testing results must be documented and shared. It is recommended that PMs contact the NIETI team (see Annex C References) to learn more about past lessons learned from CE and the opportunities to participate in future events.

##### **5.4.2.1 NATO to NATO Interoperability Testing**

Interoperability between MCCIS is obtained by implementing homogeneous software at all MCCIS sites. Any changes to operational MCCIS software is extensively tested at the MCCIS test facility. Changes to operational MCCIS software is controlled through a central configuration management process, guaranteeing common release of software to all MCCIS sites.

ACE ACCIS will follow an approach similar to the one used by MCCIS. All ACE ACCIS sites will contain identical software except for a limited amount of software required for site unique purposes. The limited site unique software will have no impact on interoperability between ACE ACCIS nodes. Changes to operational ACE ACCIS software will first be

tested in the NC3A System Test, Validation and Integration Facility (STVIF). Changes to operational ACE ACCIS software will be centrally managed by NACOSA. Through the Approved Fielded Products List (AFPL) NACOSA will control the software products allowed for installation on ACE ACCIS. The NACOSA web-site on CRONOS is at url: [www.nacosa.nato.int](http://www.nacosa.nato.int).

NATO to NATO interoperability testing becomes even simpler with the evolution of ACE ACCIS and MCCIS to the Bi-SC AIS. NACOSA will maintain a Bi-SC AIS AFPL.

#### **5.4.2.2 NATO to National Interoperability Testing**

This section provides guidance on the testing aspects that have to be taken into consideration by the National Project Manager (NPM) when connecting a National CIS system to the NATO Secret WAN.

The approach to testing is divided into two main phases: Phase 1 – Testbed testing, and Phase 2 – Site / Live testing. Both of these phases are discussed below and examples provided to aid understanding.

##### **5.4.2.2.1 Phase 1 (Testbed Testing)**

Phase 1 or testbed testing seeks to connect both the National and NATO Test and Reference Facilities (T&RF) to conduct testing, either locally or over a WAN link. The latter is the recommended option since it facilitates easy co-ordination and communication. The alternative is to have a representative portion of the National CIS connected locally to a suitable NATO T&RF.

The aim of testbed testing is to highlight potential problems that may arise during the site/live connection and resolve them before proceeding to site. The setup and configuration of the test must simulate the live connection as closely as possible.

The following areas of special concern should be taken into consideration during this test phase:

- Physical interface/presentation and LAN media.
- Simulating the WAN connection (e.g. Satellite delays, bandwidth and ‘noisy lines’).
- Packet, router/switch protocols and presentation.
- Naming conventions (e.g. O/R addresses for email).
- Addressing schemas (e.g. IP numbering).
- Security devices configured as per the live connection (e.g. firewalls and cryptographic devices).
- Software with correct patches, and configured as per the live connection.
- Information throughput across the interface.

The sub-sections below address specific areas.

##### **5.4.2.2.1.1 Management**

One of the main drivers for a successful or positive outcome to the test is the early establishment of dialogue between the NPM and Manager at the NATO T&RF. A NIETWG member will be assigned to the NPM to assist in co-ordinating all tests (Testbed and Site/Live). This NIETWG member provides a single NATO POC for all testing activities.

It is important to agree the timetable, resource provision, test objectives, assessment criteria, documentation and procedures for the test, and to assign any associated responsibilities.

For example, issues such as the safe storage of equipment at site and level of technical support required by each party need to be considered.

#### 5.4.2.2.1.2 Test Objectives

The test objectives have to be clearly defined and understood by all parties in advance of the testing to avoid any misunderstanding. This will help to define the boundary of the test and recognise any testing that exceeds this.

For example: the objective of a test may be to validate the email exchange functions between two systems, one using X.400 protocols/products and the other based on Microsoft Exchange. The test procedures or functions may include:

- Email exchange between the two systems.
- Directory update/synchronisation.
- Correct handling of forward and reply.
- Correct handling of multiple recipients.
- Blocking of non-safe file types.
- Correct handling of delivery and read report.

#### 5.4.2.2.1.3 Security

Before this stage has been reached the relevant security authorities must have agreed the connectivity design and relevant documentation. The testing should be in line with the proposed security architecture/design.

Formal approval from the security authorities may be required at this stage if classified materiel is to be used. (e.g. cryptographic devices, classified data and files).

#### 5.4.2.2.1.4 Test Procedures and Results

An unambiguous test procedure document reflecting the test objectives should be produced by the NPM, co-ordinated with the NIETWG POC, and agreed with the NATO T&RF manager well in advance of the test.

The test procedure document should include the following information:

- Introduction and Scope
- Abbreviations
- References

- Test Pre-Requisites (e.g. system status/ build, configuration, connectivity diagram)
- Test Procedure
- Test data to be collected
- Data Collection Forms (Test Result, Observation and Problem recording)

An example test procedure format for e-mail exchange can be found at Annex B:

#### 5.4.2.2.1.5 Test report

On completion of testing a report should be produced which includes:

- An Executive Summary
- Brief System description
- The Operational Requirement(s) or reference to the Operational Requirements
- System Test Configuration (e.g. physical, network, software build, addressing, naming)
- Test Timetable
- Test Objectives
- Test Procedures and results
- Additional test information (e.g. any additional testing or deviations)
- Conclusion
- Recommendation (e.g. to proceed to site/live testing taking note of agreed shortfalls)

#### **5.4.2.2.2 Phase 2 (Site/Live Testing)**

On successful completion of Phase 1 and having agreed any shortfalls with relevant authorities transition to Phase 2 can take place.

##### 5.4.2.2.2.1 Management

The NPM must be aware that at site/live testing dialogue may need to be established with a number of NATO agencies (e.g. local network support, security authorities, Users and directory manager). The assigned NIETWG POC will assist the NPM in establishing all required dialogue.

When the test connection is between 'live' or operational systems the testing has to be planned around 'quiet' periods without impacting on Operations. This requires flexibility in planning and availability of resources. There has to be sufficient confidence that testing will not impair the 'live' system(s) and all necessary actions have been taken to counter this possibility.

Any testing not covered during Phase 1 should be given careful consideration as this may be an area of risk.



The NPM, with help from the NIETWG POC, may have to reach agreement for the conduct of the test with a number of local agencies as well as policy and user areas.

#### 5.4.2.2.2.2 Test Objectives

As for phase 1

#### 5.4.2.2.2.3 Security

No form of connection should be made between the systems without the prior agreement of the appropriate security authorities. The security authorities should be made aware of any deviations from the security architecture/design/procedures and their agreement sought.

The security authorities will issue a formal approval for connection when all the pre-requisites are in place.

#### 5.4.2.2.2.4 Test Procedures and Results

As for phase 1.

#### 5.4.2.2.2.5 Test Report

As for phase 1.

The conclusion may make a recommendation for the connection to go operational or remain under development with a partial operational status.

### **5.4.3 Standards Conformance Testing**

Conformance is often defined as testing to see if an implementation meets the requirements of a standard or specification. There are many types of testing that include testing for performance, robustness, behaviour, functions and interoperability. Although conformance testing may include some of these kinds of tests, it has one fundamental difference -- the requirements or criteria for conformance must be specified in the standard or specification. This is usually in a conformance clause or conformance statement, but sometimes some of the criteria can be found in the body of the specification. Some standards have subsequent documentation for the test methodology and assertions to be tested. If the criteria or requirements for conformance are not specified and agreed upon accordingly, there can be no conformance testing.

The general definition for conformance has changed over time and been refined for specific standards. In 1991, ISO/IEC DIS 10641 defined conformance testing as "test to evaluate the adherence or non-adherence of a candidate implementation to a standard." ISO/IEC TR 13233 defined conformance and conformity as "fulfilment by a product, process or service of all relevant specified conformance requirements." In recent years, the term conformity has gained international use and has generally replaced the term conformance in ISO documents.

In 1996 ISO/IEC Guide 2 defined the three major terms used in this field.

- conformity - fulfilment of a product, process or service of specified requirements

- conformity assessment - any activity concerned with determining directly or indirectly that relevant requirements are fulfilled.
- conformity testing - conformity assessment by means of testing.

ISO/IEC Guide 2 also mentions that "Typical examples of conformity assessment activities are sampling, testing and inspection; evaluation, verification and assurance of conformity (supplier's declaration, certification); registration, accreditation and approval as well as their combinations."

Conformance tests should be used by implementers early-on in the development process, to improve the quality of their implementations and by industry associations wishing to administer a testing and certification program. Conformance tests are meant to provide the users of conforming products some assurance or confidence that the product behaves as expected, performs functions in a known manner, or has an interface or format that is known. Conformance testing is NOT a way to judge if one product is better than another. It is a neutral mechanism to judge a product against the criteria of a standard or specification." Testing products for conformance to a standard does not necessarily guarantee that the two products will interoperate even though they have both been certified as conformant.

#### **5.4.3.1 COTS Standards Conformance Testing**

Conformance testing for implementing COTS standards contained in the NCSP should be the primary responsibility of the providers of these COTS products. There are a number of commercial conformance testing organisations available to product implementers. Some examples include:

- Open GIS Consortium - testing conformance of products to OpenGIS Implementation Specifications
- W3C HTML Validation Service - checks HTML documents for conformance to W3C HTML and XHTML Recommendations and other HTML standards
- Open Group – has a family of test suites for Open Brand (provides the purchaser with a binding supplier guarantee that each registered product conforms to open standards). An example is the Open Brand for LDAP 2000.
- Web Services Interoperability Organisation (WS-I) – WS-I is an open, industry organisation chartered to promote Web services interoperability across platforms, operating systems, and programming languages (see <http://www.ws-i.org/> for further info)

The NIETI team maintains a list of commercial organisations that perform conformance testing for COTS based products. In addition the NIETI team can advise Program Managers on whether or not a specific COTS product has a certificate of compliance to the standard it has implemented.

#### **5.4.3.2 Non-COTS Standards Conformance Testing**

Non-COTS standards are defined as any standard that contains NATO unique extensions to a commercial standard (e.g. STANAG 4406) or a NATO developed standard (e.g. STANAG 5516). All of these are based on GOTS, NOTS and MOTS products. Since commercial organisations performing conformance testing are not likely to have test suites/procedures available for NATO STANAGs, NATO must rely on NATO (e.g. Message Security Demonstrator Program testbed) or National (e.g. Joint Interoperability Test Command) facilities. If neither NATO or National facilities have test suites/procedures available for a particular STANAG, then NATO must decide on whether or not to fund or sponsor the development of the required test suites/procedures. Only STANAGs that have been promulgated are eligible for this NATO funding.

The NIETI team maintains a database of NATO and National test facilities with their corresponding capabilities. The NIETI team also maintains a list of products conformant with STANAGs.

#### **5.4.4 Integration Testing**

Integration testing is required to provide PMs with confidence that software will correctly install/uninstall and that the installed software will successfully run on the intended platform (i.e. W2K or UNIX). Although the following is mainly oriented to PMs dealing with NATO Common Funded Systems, National PMs may also find the information of value when developing National C3 Systems.

##### **5.4.4.1 Windows Environment**

Microsoft has developed “The Application Specification for Windows 2000”<sup>7</sup> to help software developers create reliable and manageable software. This application specification has two versions: one for desktop applications and the other for distributed applications. The Application Specification provides the technical details required for software to achieve the Certified for Windows Logo. If software developers believe that their software does not require the Certified for Windows Logo, they can submit their software for testing to the less stringent requirements of Compatibility with Windows 2000 test, which is based on Microsoft’s “Compatibility Specification for Windows 2000”.

Both the Certified for Windows Logo and Compatible with Windows 2000 tests are performed by VeriTest (<http://www.veritest.com>), which has test labs in Los Angeles, Paris and Ballina, Ireland. W2K software for the NCOE should have the Certified for Windows Logo because of the importance of the core software. Since most of this core software will be COTS software, the software vendor should provide their Certificate before the software is included in the NCOE Basket of Products. For Functional Service software, the PM will have to decide on whether to verify the software for either Compatible with W2K test or Certified for Windows test. For additional information pertaining to the W2K application specification, see Annex E.

---

<sup>7</sup> Microsoft is expected to develop similar documentation for future version of Windows.

Before deploying any new W2K software in NATO Common Funded systems, further integration testing will have to be performed in the Test & Integration Facility (TIF) located at the NC3 Agency, The Hague, NL.

#### **5.4.4.2 UNIX Environment**

For details pertaining to the installation, integration and testing procedures for all NATO common funded UNIX based operating system platforms please see section 3.0 of the MCCIS Software Specification dated July 15, 1999. Software approved for MCCIS may be found in MCCIS Release 4.3 dated 9 May 2002 or by contacting [uds@saclant.nato.int](mailto:uds@saclant.nato.int).

## **6. USAGE PHASE (O&M)**

### **6.1 INTRODUCTION**

This section covers the issue of lifecycle management of NATO CIS (Communication Information System(s)) in operation (in the usage phase), providing an overall view of the Configuration Management (CM) Policy to be used with fully or partly common-funded NATO CIS. This policy is required due to the complexity and specialised nature of CIS, with a need to cater for the situation where:

- CIS facilities and capabilities are undergoing change continuously due to rapidly evolving operational needs and the increasing dependence on commercial technology (NCOE BoP).
- Changes may occur in a system's operational fielded configuration at the same time as that system is undergoing further development and new sub-systems are added through a rapid evolutionary acquisition process.
- CIS are fielded NATO wide and require linkage between common core network and services and a heterogeneous family of applications and local networks. The distributed nature of such systems increases overall complexity and requires clearly defined management arrangement.
- Sub-systems acquired by different Host Nations (HN) have to be integrated into a well-functioning "family of systems".
- Management and co-ordination across a wide variety of NATO and National authorities at a number of levels is required during the CIS life-cycle.

For further information on NATO CM there are a number of NATO documents, with the following hierarchy:

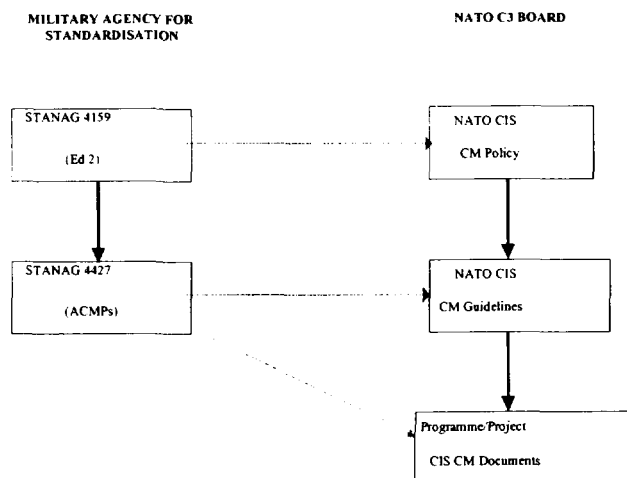


Figure 6-1: NATO CM-related Documents

CM for NATO software based systems is also addressed in the NATO Software Management Concept (AC/317-D/67) and the NATO Software Management Policy (AC/317-D/70).

The related topics are:

- Support phases of the operation of CIS themselves
- Support phases of related standards in NCSP
- Support phases of related products (in particular those in the NCOE BoP)

Since this phase covers the usage, operation and maintenance of the products, there would be updates in the NTV-1 and NTV-6 constructed in the previous phases when there are changes in the specifications.

There exists a strong dependency between the management of the lifecycle of NATO CIS and the updating of the NC3TA. A release management strategy has been established for the NCOE BoP (NC3TA Volume 1 and 5) and for the Bi-SC AIS and National CIS (Annex C).

## **7. SUPPORT**

### **7.1 INTRODUCTION**

The NC3TA Implementation Handbook identifies requirements to support planners, architects, designers, implementers, maintainers and program managers in performing their respective responsibilities. Support covers methodology, dissemination of information, tools and training.

### **7.2 METHODOLOGY**

The NC3TA-IHB identifies in Annex A the templates that need to be filled out by project managers and architects but doesn't provide a methodology how to do this. It is up to the project managers and architects to choose appropriate methodologies that fit their needs. There is a need for a methodology to fill out the NC3TA templates from Annex A, and also more generally for all Operational, System and Technical View templates in the NATO C3 System Architectural Framework. Methodologies will be required for Overarching, Reference and Target Architectures.

### **7.3 DISSEMINATION OF INFORMATION**

There is a plan for a WEB-based repository that provides access to the NC3TA - and NATO C3 Architectural Framework templates. This WEB page will also be used e.g. to make the tools available to develop architectures and publish awareness briefings.

### **7.4 TOOLS**

Tools for supporting the use of specific architectural frameworks are commercially available. The applicability of these tools to the templates as identified in the NC3TA has to be explored.

Other non-commercial tools may support specific aspects of the NC3TA-IHB. The web-enabled tool GfIP supporting the Interoperability Profile Selection and Development Process (see 5.2.6) is available to implement one of these aspects (see Annex D).

## **7.5 TRAINING FOR USING THE NC3TA**

Currently no formal training is available in the use of the NC3TA, however, it is planned that for program managers a course will become available through the NATO CIS school by 2004.



## **ANNEX A NC3TA COMPLIANCE TEMPLATES**

The NC3TA Compliance Templates are each dealing with compliance issues at the different phases of the project life-cycle. The templates should be filled in and updated at the relevant project milestones throughout the life-cycle in order to ensure that adequate visibility of the NATO Technical views is maintained within the NIE context. See also NIMP VOL II Architectural Framework for all NIE relevant templates.

As a minimum, the Host Nation should deliver the following templates as milestones are achieved:

NATO System View Template 11 (NSV-11) C3 Interoperability Requirements  
Interoperability Requirements defined through sub-degrees of interoperability should be defined at the end of the Concept Phase as a supporting template and provided with the CP.

NATO System View Template 12 (NSV-12) Functional Configurations.

Functional Configurations (FC) should be defined for the Reference Architecture during the project's Definition Phase as an essential template. A first architectural description using FCs should be developed in the Reference Architecture at the CP stage. This will allow defining the related Technical and Software Configurations that include the appropriate standards and products (see NTV-3 and 4) for the Target Architecture at the TBCE stage.

NATO Technical View Template 1 (NTV-1) Project Standards Profile.

Project NCSP Standards Compliance as an essential template should be part of the TBCE and the Target Architecture in the Procurement Phase, and if necessary updated to be issued with the Statement of Work (SOW),

NATO Technical View Template 2 (NTV-2) Standards Technology Forecast.

The Reference Architecture should provide a technology forecast as an supporting template to indicate what sort of technology might be expected within a five years timeframe. The Target Architecture should indicate what standards technology is foreseen in the coming 2 year timeframe.

NATO Technical View Template 3 (NTV-3) Technical Configurations.

Technical Configurations are essential templates and are derived from the project's Functional Configurations (see NSV-12) and contain the standards that are required for the functional services within the Functional Configurations.

NATO Technical View Template 4 (NTV-4) Software Configurations.

Software Configurations are essential templates and are derived from the project's Technical Configurations (see NTV-3) and contain the products that are required to implement the standards within the Technical Configurations.

NATO Technical View Template 5 (NTV-5) Interoperability Profile Selection/Development.

Both Internal and External Interoperability Profiles should be selected or defined as part of the Target Architecture in the Procurement Phase as supporting templates.

NATO Technical View Template 6 (NTV-6) NCOE Product Selection Report.

NCOE products with a selection report should be provided in the Procurement Phase as essential templates before the RFQ/IFB is released and/or before the contract is awarded.

**A.1 C3 INTEROPERABILITY REQUIREMENTS (NSV-11)**

The C3 Interoperability Requirements Template NSV-11 is an supporting template that is to be used for the development of the System View of the Reference Architecture.

**C3 INTEROPERABILITY REQUIREMENTS TEMPLATE**

<b>IDENTIFICATION</b>	Number:	Status:	Date <sup>8</sup> :
	Priority <sup>9</sup> :	Completion date <sup>10</sup> :	

<b>ORIGINATOR</b>	Organisation/Command:
-------------------	-----------------------

---

<sup>8</sup> DD/MM/YY

<sup>9</sup> If the IOR is directly related to a C2 requirement from the Bi-SC C2 Plan – Part 2, the same priority as the one assigned to the underlying C2 requirement is to be applied.

<sup>10</sup> If applicable. For those IORs taking part of a whole document, project, etc, the completion date for the document or project should also apply for the IOR.

Department /Division:		Section/Office:		
<i>Action Officer</i>	Rank:	Name:	Nat:	SVC:
Tel No:		Fax No:	E-mail:	

<b><i>TITLE</i></b>	

<b><i>DESCRIPTION</i></b>	
<b><i>SOURCE</i></b>	

☐ Bi-SC C2 Plan –Part 2- C2 Requirements

☐ MOR

☐ CP

☐

☐

## ***SUPPORTED OBJECTIVES***

***DCI tasks***

***NC3O G&O***

☐ PCNCEP CIS Requirement Document

☐ Project

☐ TBCE

☐☐

<b><i>JWID 200x objectives</i></b>	
<b><i>Lessons learned</i></b>	

Degrees and Sub-degrees of interoperability		
<input type="checkbox"/> 1	<b>Unstructured Data Exchange</b>	Involves the exchange of human-interpretable unstructured data such as the free text found in operational estimates, analysis and papers.
<input type="checkbox"/> 1.A	<b>Network Connectivity</b>	Network connectivity can range from a simple transport line for file transfer or basic email connecting to non-NATO systems, to full connectivity with services required by the higher sub-degrees. Network connectivity is normally provided by the NATO network infrastructure. In selecting this sub-degree, the appropriate supporting network domain infrastructure should be identified.
<input type="checkbox"/> 1.A.1	Internetworking	All LAN, MAN, WAN Connections
<input type="checkbox"/> 1.A.2	Secure Internetworking	Secure LAN, WAN, WAN Connections.
<input type="checkbox"/> 1.A.3	Packet Switch WAN	Connecting to NIDTS/PTT Packet Network
<input type="checkbox"/> 1.A.4	Circuit Switch WAN	Connecting to NCN, National, Commercial Switched Network
<input type="checkbox"/> 1.A.5	Remote Terminal	Interactive computer session from remote location
<input type="checkbox"/> 1.A.6	TADIL Comms	Communications for Tactical Link 11, 16 and 22 Data Interchange
<input type="checkbox"/> 1.A.7	SATCOM	Connecting to UHF and EHF Satellite Comms



<input type="checkbox"/> 1.A.8	Telephone
<input type="checkbox"/> 1.A.9	Telefax
<input type="checkbox"/> 1.A.10	Radio
<input type="checkbox"/> 1.A.11	Cable
<input type="checkbox"/> 1.B	Basic Document Exchange
<input type="checkbox"/> 1.C	Basic Informal Message Exchange
<input type="checkbox"/> 2	<b>Structured Data Exchange</b>
<input type="checkbox"/> 2.A	Enhanced Informal Message Exchange
<input type="checkbox"/> 2.B	Enhanced Document Exchange
<input type="checkbox"/> 2.C	Network Management

	Analogue or digital telephone. Includes voice over IP, (secure) GSM.
	Analogue, digital or secure facsimile.
	Connecting to HF, VHF and UHF Radios. w/wo voice encoding.
	Serial, parallel and optical cable connections
	Includes services for Office Automation, character sets/alphabets, file archiving, file compression.
	Includes services for text only messages and basic directory services.
	Involves the exchange of human-interpretable structured data intended for manual and/or automated handling, but requires manual compilation, receipt and/or message dispatch.
	Includes services for informal multimedia email, enhanced directory services, plus relevant associated communications upper layers.
	Includes services as in 1B plus hypertext, graphical/sound image data interchange, moving image and audio/visual data interchange, file compression, page description and version management.
	Includes services for network monitoring and management.

<input type="checkbox"/> 2.D	Map Overlays/Graphics Exchange	Includes services for geo-data, overlay formats, and military symbology.
<input type="checkbox"/> 2.E	Directory Services	Includes services for directory, directory schema, and shadowing/chaining protocols.
<input type="checkbox"/> 2.F	Web Access	Includes services for hypertext transfer, on-line publishing, bulletin board services, Web authentication and access control mechanisms.
<input type="checkbox"/> 2.G	Multi-Point Applications	Includes services such as audio/video teleconferencing, white-boarding and application sharing
<input type="checkbox"/> 2.H	Data Object Exchange	Includes services for exchange of formatted data within messages using e.g. MTFs or XML.

<input type="checkbox"/> 3	<b>Seamless Sharing of Data</b>	Involves the automated sharing of data amongst systems based on a common exchange model.
<input type="checkbox"/> 3.A	Formal Message Exchange	Includes services for formal messaging (incl message security services, labelling syntax, semantics and MTFs).
<input type="checkbox"/> 3.B	Common Data Exchange	Includes services for DBMS.

<input type="checkbox"/> 3.C	System Management
<input type="checkbox"/> 3.D	Secure Systems Management
<input type="checkbox"/> 3.E	Security Management
<input type="checkbox"/> 3.F	Real-time Data Exchange
<input type="checkbox"/> 4	<b>Seamless Sharing of Information</b>
<input type="checkbox"/> 4.A	Common Information Exchange
<input type="checkbox"/> 4.B	Distributed Applications

	Includes services for network monitoring and management.
	Includes services for secure systems and management of all systems and network resources.
	Includes services such as public key infrastructure (PKI).
	Includes services for exchange of data using tactical links in real time.
	An extension of degree 3 to the universal interpretation of information through data processing based on operating applications.
	Includes services for the management of information defined in the NATO corporate data model, including security information.
	Includes services for distributed computing (distributed process, time, file, print and transaction services), object interfaces and object middleware if relevant, database to database replication, workflow, alert.

## **A.2 FUNCTIONAL CONFIGURATIONS (NSV-12)**

### **A.2.1 Introduction**

The Functional Configurations template (NSV-12) is an essential template for the development of the System View of the Reference Architecture. Architecture Compliance with the NC3TA Functional Configurations (FC) as defined in the NC3TA Volume 2 should be applied during the project's Definition Phase. An architectural description using FCs and their functional interfaces should be developed in the Reference Architecture at the CP stage. This will allow defining the related Technical Configurations (see NTV-3) that contain the appropriate standards, and Software Configurations (see NTV-4) that include the products for the Target Architecture at the TBCE stage.

The list below shows the current FCs. Most of these FCs have been refined into potential child FCs in order to amplify their functional role:

1. User Terminal/Device,
2. User Workstation,
3. Administration Workstation,
4. Network Server,
  - a Network Controller
  - b Domain Name Server
  - c Enterprise Directory Server
  - d Key Distribution Server
5. Messaging and Communications Server,
  - a NATO Messaging Server
  - b Email Server
  - c "Instant messaging" Server
  - d Communications Server (TADILs, Satellite, Fax, VHF,...)
6. Document Management Server,
  - a Office Automation Server,
  - b Index Server (search engine)
  - c Document Handling and Workflow Server

## 7. Web Portal/Application Server,

- a Web Portal
- b Mission (/Functional) Application Server

## 8. Database Server

- a Geo(graphic) Database
- b Mission (/Functional) Area Database

These configurations constitute an initial, albeit not all-inclusive list of FCs. This list will be validated and/or updated in future versions of the NC3TA. For future consideration communications FCs such as directory servers and routers, and security-related FCs such as boundary controllers (firewall, guard, proxy-server) could be considered.

The Reference Architecture should define the appropriate FCs by using the form below and taking the FC models from NC3TA Volume 2, and adapting them to the required functionality. The functionality of each FC and the functional interfaces between FCs should be specified. Figure A-1 below gives an overview of the major FCs. In order to improve the reuse of FCs within future architectural developments, each new FC will need to be registered as a template/model within the NC3TA Volume 2. Therefore the filled-out FC templates for new FCs, together with an RFCP should be sent to the ISSC Secretary (see address at chapter 1.5).

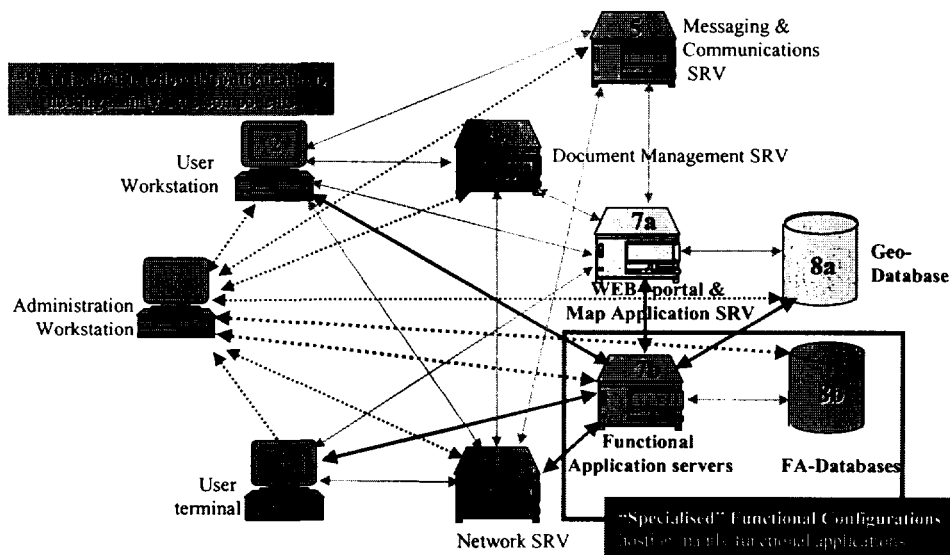


Figure A-1: Functional Configurations connected through Functional Interfaces.

**A.2.2 Functional Configuration Template**

<b>NSV-12</b>	<b>FUNCTIONAL CONFIGURATION (FC) TEMPLATE</b>  <b>(to be filled in at Definition Phase for the Reference Architecture)</b>				
<b>Project Title</b>					
<b>Project POC</b>	<b>Name:</b>	<b>Address:</b>		<b>Tel/Fax/Email</b>	
<b>FC Title</b>					
<b>FC Type</b>  Note: Chose existing type, otherwise, create new child FC under one of the main categories, or create a new category.					
<b>Short Description</b>  Note: Describe FC's generic and specific functionality such as security control.					
<b>FC Services at:</b>          Note: Describe the application services in functional terms.	<b>Foundation Services</b>			<b>Application Services</b>	
	<b>Network Services Layer</b>	<b>Kernel Services Layer</b>	<b>Infrastructure Services Layer</b>	<b>Common Support Application Layer</b>	<b>Specific Mission Application Layer</b>



**Functional  
Interface**

Note: Describe the functional interface with other FCs in terms of required interoperability services (e.g. email, authentication) and the required quality and quantity attributes (e.g. nr of messages, security credentials) using the NSV1 (a-d), NSV3 and NTV1 templates.

### **A.3 PROJECT STANDARDS PROFILE (NTV-1)**

The Project Standards Profile (NTV-1) is an essential template for the Technical View of the Target Architecture. A project overview or profile of NCSP Standards Compliance should be part of the TBCE and the Target Architecture in the Procurement Phase, and if necessary updated to be issued with the Statement of Work (SOW). This template should have the following contents:

<b>SERVICE AREA</b>	<b>CLASS</b>	<b>MANDATORY STANDARDS</b>	<b>NON-NCSP STANDARDS</b>	<b>Derived from Interoperability Profile</b>	<b>REM</b>
See chapter 3 Volume 4 (NCSP)	See Volume 4 (NCSP)	See Volume 4 (NCSP)	1. Understood as: Not incl. in NCSP or incl. in NCSP as mandatory or emerging but with different reference. 2. The ref. to the std. (if any) or product name. 3. Ref. to the document providing the rationale for support of non-NCSP standard choice, 4. Indication of reqmt. for NCSP Change Request	Y= Yes + nr N= No	Reason for selecting standard

#### **A.4 STANDARDS TECHNOLOGY FORECAST (NTV-2)**

The Reference and Target Architectures should provide a Standards Technology Forecast to describe the emerging technology standards relevant to the architecture. The Standards Technology Forecast (NTV-2) is a supporting template for the development of the Technical View of the Reference and Target Architectures. The Reference Architecture should provide a Standards Technology Forecast to indicate what sort of technology might be expected within a five years timeframe. The Standards Technology Forecast for the Target Architecture should cover a 2 year period, addressing the emerging standards. NC3TA Volume 2 contains a section on emerging technologies as a point of reference.

The table below shows an example of the Standards Technology Forecast. All entries in the figure are for illustration only.

<b>SERVICE AREA</b>	<b>CLASS</b>	<b>MANDATORY STANDARDS</b>	<b>EXPECTED BY T0+ 2 YEARS</b>	<b>EXPECTED BY T0 + 5 YEARS</b>
<b>COMMUNICATIONS</b>	<b>Messaging</b>	STANAG 4406 edition 1		
		SMTP (RFC 821, 1869, 1870)	eSMTP (RFC 1891, 1985, 2034, 2197, 2487, 2554)	
		POP3 (RFC 1939: 96)	IMAP4 (RFC 2060: 96)	

## **A.5 TECHNICAL CONFIGURATIONS (NTV-3)**

### **A.5.1 Introduction**

The Technical Configurations template (NTV-3) is an essential template for the development of the Technical View of the Target Architecture. An architectural description using TCs and their interoperability profiles should be developed in the Target Architecture at the TBCE stage. This will allow defining the related Software Configurations (see NTV-4) that contain the appropriate products.

### **A.5.2 Technical Configuration Template**

NTV-3	<b>TECHNICAL CONFIGURATION (TC) TEMPLATE</b> <b>(to be filled in at Procurement Phase for Target Architecture)</b>				
TC Components and Standards at:      Note: attach for each required component a detailed description	Network Services Layer	Kernel Services Layer	Infrastructure Services Layer	Common Support Application Layer	Specific Mission Application Layer
Internal Interoperability Profiles (IIP) between TC and:   Note: Attach for each IIP a detailed description	User Desktop: <specify>	User Desktop: <specify>	Server: <specify>	Server: <specify>	Server: <specify>

<b>IIP-Number</b>  Note: Use numbering as follows: IIP<TCnr>-<TCnr>		
<b>External Interoperability Profile between TC and:</b>  Note: Attach for each EIP a detailed description <b>EIP-Number and Basic Functionality</b>  Note: Use numbering as follows: EIP<TCnr>-<TCnr>	<b>National User Desktop:</b> <specify>	<b>National Server:</b> <specify>

National Server: <specify>	National Server: <specify>	National Server: <specify>

## **A.6 SOFTWARE CONFIGURATIONS (NTV-4)**

### **A.6.1 Introduction**

The Software Configurations template (NTV-4) is an essential template for the development of the Technical View of the Target Architecture. An architectural description using SCs, their software interfaces should be developed in the Target Architecture at the IFB/SOW stage. Also the SC should define the segments and their constituting products.

### **A.6.2 Software Configuration Template**

<b>NTV-4</b>	<b>SOFTWARE CONFIGURATION (SC) TEMPLATE</b> <b>(to be filled in at Procurement Phase for Target Architecture)</b>				
<b>SC Products in:</b>    Note: indicate software version number and standard(s) which are covered by the software package	Network Services Layer	Kernel Services Layer	Infrastructure Services Layer	Common Support Application Layer	Specific Mission Application Layer
<b>Segments</b>  Note: Describe the products that constitute the different segments.	Segment 1	Segment 2	Segment 3	Segment 4	Segment 5

Interfaces	Internal	Internal	External	External	External

Note: describe interfaces in terms of APIs embedded in products or as separate products. Mention the standards supported and possible parameter settings.



## **A.7 INTEROPERABILITY PROFILE SELECTION/DEVELOPMENT (NTV-5)**

The Interoperability Profile Selection/Development template (NTV-5) is a supporting template for the development of the Technical View of the Target Architecture.

### **A.7.1 Selection of Profiles**

Most of the communication protocols are included within OTS Communication Software and therefore no profiling is required. However, the most popular used communication service – messaging – raises some problems within the NATO community. On the one hand, the messaging interoperability among Nations is based on the X.400 MTA-MTA protocol suite. On the other hand, within the end system domain, SMTP or proprietary protocols (e.g. Microsoft or Lotus Notes) are used. Within a W2K domain SMTP is used for clear messages, signed messages as well as encrypted messages.

So called connectors, placed in the Messaging Transfer Agent (MTA) convert end system protocols into X.400 MTA-MTA protocols. The following figure depicts the W2K messaging interoperability scenario:

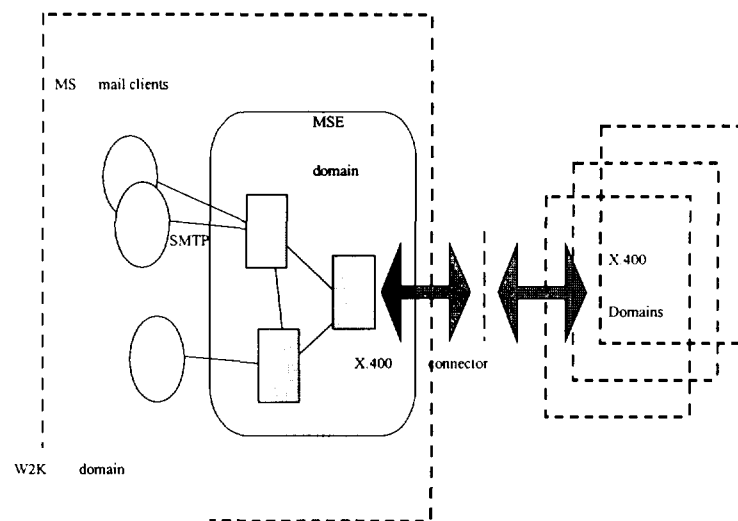


Figure B-1: W2K Interoperability Scenario

SMTP messages composed by the MS-Outlook or Outlook-Express client will be forwarded to the corresponding MS Exchange Server. The Exchange Server placed at the interoperability boundary is configured as an X.400 Connector, which maps the SMTP message format (MIME) into an X.400 Message. All attached data objects are conveyed unmodified as X.400 specific content type and vice versa. SMTP messages can be received and processed in SMTP and X.400 messaging domains. This basic messaging scenario requires particular attention in the context with security.

The three tables below contain Data Interchange, Communications and Security External Interoperability Profiles that are mandatory for use between NATO systems and between NATO

and National systems. Internal Interoperability Profiles that are mandatory within NATO systems only, will be defined at a later stage.

<b>Data Interchange Profile</b>	<b>Between FC-FC<sup>11</sup></b>	<b>Service or Standard</b>	<b>Communication or Standard</b>	<b>Service</b>	<b>Profile ID<sup>12</sup></b>
<b>Technical/business data</b>	1-7 a/b 2-5,2-6,2-7 a/b,3-all (WBEM)	HTML objects	HTTP		WIP-http
	7a-7b; 7b-7b	XML objects	HTTP		WIP-xml
	2-5;2-6;6-7a	MS-Office Files	FTP, SMTP, MMHS		OTS
	2-5;2-6;6-7a	PDF/RTF Files...	FTP, SMTP, MMHS		OTS
<b>Graphical Files</b>		See Technical/business data			
<b>Audio/Video</b>	2-5,5-5	H323			
<b>Tactical Digital Data</b>		TADILS	Link 11. STANAG 5511		STANAG 5511 annex B
			Link 16. STANAG 5516		STANAG 4175 edition 1.
			Link 11, 16, 22 UHF.		STANAG 4372 (Saturn).
			Link 22 HF		STANAG 4444 (Slow hop ECCM)
			Link forwarding between Link 11/11B and Link 16		STANAG 5616
<b>Tactical Message Data</b>	2-5; 5-5	Military Message Text Formats, ADatP-3	MMHS, STANAG 4406		STANAG 5500

<sup>11</sup> For the numbers of the Functional Configurations (FC) refer to NC3TA Vol 2 or figure 4-2.

<sup>12</sup> Profile ID refers to either proprietary OTS profiles that are available within the products, or an identifier for which more information can be found in NC3TA Volume 3 Annex A.

<b>Communications Profile</b>	<b>Between FC-FC</b>	<b>Service or Standard</b>	<b>Communication or Standard</b>	<b>Service</b>	<b>Profile ID</b>
<b>Messaging</b>	2-5 5-5	Informal message	SMTP/X.400 (based on QoS)		MIP-SMTP
	2-5; 5-5	Formal message	MMHS, STANAG 4406		MIP-MTA AMH1x, AMH2x, AMH9x
<b>Directory</b>	4-4	schema	ACP 133 B		DIP-DS
	2-4	access, LDAP/DAP	ACP 133 B		DIP-LDAP
	4-4	chaining, DSP	ACP 133 B		DIP-DAP DIP-DSP
	4-4	replication, DISP	ACP 133 B		DIP-DISP
	3-4	management, DOP	ACP 133 B		DIP-DOP
<b>Name Services</b>	1-4,2-4,4-4	DNS, IETF STD-13	TCP/IP		Bind version 8.2 or later
		Naming Addressing	STANAG 4250 part 3, TCP/IP		NACOSA Operating Instructions A-03-06
			ISO 7498-3, OSI		NACOSA OI A-03-07

<b>Security Profile</b>	<b>Between FC-FC</b>	<b>Service or Standard</b>	<b>Communication or Standard</b>	<b>Service</b>	<b>Profile ID</b>
<b>Secure Messaging</b>	2-5,5-5	S/MIME encapsulation	SMTP, rfc 2633		MIP-S/MIME
	2-5,5-5	S/MIME interoperable PCT	X.400		MIP-S/MIME-X.400 Wrap
<b>Data Object Encapsulation</b>	1-7a/b 2-5,5-5 2-6,6-6 2-7a/b	CMS for files	SMTP, X.400, FTP		MIP-S/MIME-X.400 Transport
<b>Directory</b>	4-4	PKI schema	X.500, X.509		SIP-CRDS
<b>Secure Networking</b>	R/R (R:router)	IP packets	IPSec		SIP-IPSEC
<b>Hypertext Transfer</b>	1-7 a/b	HTML, XML	SSL		WIP-SSL
	2-7a/b				

<b>Public Infrastructure Interactions</b>	<b>Key</b>	4-4	certificate repository directory schema		SIP-CRDS
		4-4	certificate policy		SIP-CPO
		4-4	certificate revocation list		SIP-CRL
			cross certification		SIP-CROSSC
		all-4	certificate request	SIP-SSL	SIP-CRQ
		4-all	certificate response	SIP-SSL	SIP-CRE

### A.7.2 Definition of Profiles

The Structure of Profiles is defined in NC3TA volume 3 and will be used within this template.

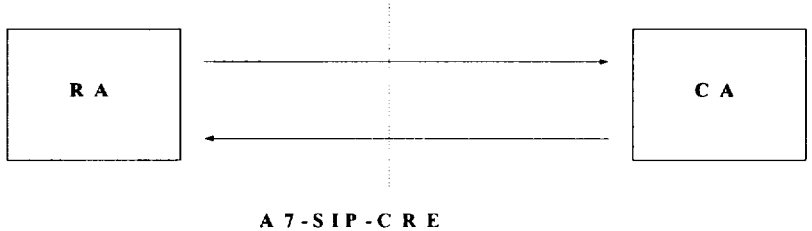
Profile Title	The title characterises the intended service of the profile, e.g. Military Message Handling System - Common Messaging
Profile Identifier	Unique Identifier within the NATO Standard Profiles
Profile Type	e.g. Messaging  Interoperability Profile – MIP
Scenario Description	Short description of the function of the profile and its relationship within a profile-set required for a particular system, e.g. Military Message Handling System
Profile Scenario	Figure depicting interacting entities and profiles required between two Functional Configurations
Protocol Set	Layered set of protocols required for the particular profile
Reference Document	List of additional documents and standards required for the specification of the profile
Implementation Details	This is a container for additional information required for the proper implementation of a profile. This may be the feedback of real projects or PM's experiences.

### **A.7.3 Characterisation of Profiles**

In addition a characterisation of profiles is included to highlight the properties of a particular profile. It serves to provide search patterns for a potential tool to support the selection process for appropriate profiles. The characterisation uses the classification schema prescribed in NC3TA Vol2, Architectural Descriptions and Models (ADaM), and adopts different views each providing different key words.

ADaM Classification	<ul style="list-style-type: none"> <li>• IT-Service (Data interchange, Infrastructure , Security)</li> <li>• Class</li> <li>• Sub-degree of Interoperability</li> </ul>
Operational View	<ul style="list-style-type: none"> <li>• Local processing of data</li> <li>• Remote processing of data</li> <li>• Access to data</li> <li>• Send data</li> <li>• Receive data</li> <li>• Exchange data</li> <li>• Connection mode of operation (session)</li> <li>• Connectionless mode of operation (atomic operation)</li> </ul>
Configuration View	<ul style="list-style-type: none"> <li>• Peer-to-Peer configuration</li> <li>• Multi-peer configuration</li> <li>• Applicable in public network environments</li> <li>• Applicable in private network environments</li> </ul>
Security View	<ul style="list-style-type: none"> <li>• Integrity</li> <li>• Authentication</li> <li>• Confidentiality</li> <li>• Access control</li> <li>• Non-Repudiation</li> <li>• Transient protection of data</li> <li>• Persistent protection of data</li> </ul>
Miscellaneous	<ul style="list-style-type: none"> <li>• Particular peer requirements</li> <li>• Quality of Service requirements</li> </ul>

**A.7.4 Example Profile for Certificate Request**

Profile Title	Certificate Request - PKI Interactions	
Profile Identifier	A6-SIP-CRQ	
Profile Type	Security Interoperability Profile - SIP	
Scenario Description	<p>The Ax-SIP-CRy set of profiles is applicable to Registration Authorities (RA) to request a certificate from a Certification Authority (CA) and provide users with requested certificates. The service characteristic of this profile is CL-mode (connectionless). The reason for is the intervening of a security administrator issuing and signing the requested certificate. The expected response is profiled in a different profile (A7-SIP-CRE).</p> <p>This A6-SIP-CRQ Profile specifies the structure and options of a certificate request and the communication service used for the transfer of the request to the appropriate certification authority.</p>	
Profile Scenario	<p style="text-align: center;"><b>A 6 - S I P - C R Q</b></p>  <pre> sequenceDiagram     participant RA     participant CA     RA-&gt;&gt;CA: A 6 - S I P - C R Q     CA--&gt;&gt;RA: A 7 - S I P - C R E </pre> <p style="text-align: center;"><b>A 7 - S I P - C R E</b></p>	
Protocol Set	<b>Layer</b>	<b>Protocols/services</b>
	Application Layer	NATO-PKCS10-RQ <sup>13</sup>  https <sup>14</sup>
	Transport Layer	TCP/IP
Reference Document	<p>PKCS#10, Certification Request Syntax Standard</p> <p>ITU-T X.509 v3 Certificates and Revocation Lists</p>	

<sup>13</sup> This document contains the definition of options and parameters of the PKCS#10 basic standard to be done by the appropriate NATO body.

<sup>14</sup> An alternative profile may use messaging as communication services.

## **A.8 NCOE PRODUCT SELECTION REPORT (NTV-6)**

The NCOE Product Selection Report template (NTV-6) is an essential template for the development of the Technical View of the Target Architecture. NCOE products with a selection report should be provided in the Procurement Phase before the RFQ/IFB is released and/or before the contract is awarded. These products should be selected from the NCOE Basket of Products (BoP). See also chapter 5.3. If products do not exist in the BoP then selection of products should follow the selection procedure as defined in the NC3TA Volume 5. If products need to deviate from those in the current BoP, a waiver procedure needs to be applied (see 5.3.2).

SERVICE AREA	CLASS	MANDATORY STANDARDS	NON-NCSP STANDARDS	TYPE OF PRODUCT	PRODUCT SELECTION	PRODUCT QUANTITY	REM
See chapter 3 Volume 4 (NCSP)	See Volume 4 (NCSP)	See Volume 4 (NCSP)	<p>1. Understood as: Not incl. in NCSP or incl. in NCSP as mandatory or emerging but with different reference.</p> <p>2. In addition. the ref. to the std. (if any) or product name</p> <p>In other cases:</p> <p>Ref. to the document providing the rationale for support of non-CSP standard choice,</p> <p>Indication of reqmt. for NCSP Change Request</p>	<p>Category:</p> <p>1=NCOE BoP</p> <p>2=Sole Source</p> <p>3=To Be Selected</p> <p>4=Compatibility with Existing Product Line</p>	<p>Is the product selected from the BoP?</p> <p>Is the product selected using the NCOE OTS Product Selection Method</p>	Indication of the number of licences (server and client) to be potentially procured, or updated.	Reason for selecting product (Cat 1,2,..)



## **ANNEX B      EXAMPLE TEST PROCEDURE**

<b>Step</b>	<b>Input/Action</b>	<b>Expected Result/Output</b>	<b>Pass / Fail</b>	<b>Comments</b>
	<b>To prove that only the agreed file types can be exchanged between XXXX and the Interconnecting System and XXXX provides all expected Delivery and Read reports.</b>			For definition of the Safe / Non Safe file types, please refer to the specific Interface Test Specification for this interconnection.
1.	Exchange the file types as listed in Table 3 between XXXX and the Interconnecting System and vice versa. Record the results in Table 3.	Agreed file types are exchanged, non-safe blocked. Delivery and Read reports are provided as expected. Attachment can be read by Interconnecting System.		

Step	Input/Action	Expected Result/Output	Pass / Fail	Comments
2.	Enter any additional file types that require testing between XXXX and the Interconnecting System in table 4. Record the results in Table 4.	Agreed file types are exchanged, non-safe blocked. Delivery and Read reports are provided as expected. Attachment can be read by XXXX.		
3.	Exchange an IPM with a safe file type attachment between a remote XXXX Site and the Interconnecting System.	IPM received by the External System. Delivery and Read reports are provided as expected.		
	<b>Directory Exchange</b>			
4.	Modify the Common Name of a XXXX user in the XXXX X.500 Directory then Create and transmit a XXXX Address List to the Interconnecting System.	The Interconnecting System receives the Address List and loads it into its Directory.		
5.	The Interconnecting System sends an email to the XXXX user with the modified Common Name.	The modified XXXX user receives the message from the External System.		

Step	Input/Action	Expected Result/Output	Pass / Fail	Comments
6.	The Interconnecting System modifies a users e-mail Address / Common Name and sends the modified address list to XXXX.	XXXX receives the modified Address List from the Interconnecting System.		
7.	The Address List is loaded into the XXXX X.500 Directory and an IPM is sent to the modified user's email address.	The Modified user on the external system receives an XXXX email.		
	<b>Correct handling of Forward and Reply.</b>			
8.	The Interconnecting System forwards an E Mail with a Safe File Type attachment to XXXX	XXXX receives the message from the external system and the Safe File Type attachment can be read.		
9.	The XXXX user replies to the message and attaches a CSV file.	The external system receives a reply to the message and the CSV file can be read.		

Step	Input/Action	Expected Result/Output	Pass / Fail	Comments
10.	The XXXX user forwards an email with a Safe File Type attachment to the External System.	The External System receives the message from XXXX and the Safe File Type attachment can be read.		
11.	The External System user replies to the message and attaches a CSV file.	The XXXX user receives a reply to the message and the CSV file can be read.		
	<b>Correct handling of multiple recipients</b>			
12.	The XXXX user sends an IPM with a Safe File Type attachment to 2 Action Addressees and One Copy Addressee.	The External System Addressee and Copy Addressees receive the e-mail and attachment.		
13.	The External System user sends an IPM with a Safe File Type attachment to 2 Action Addressees and One Copy Addressee to the XXXX Role User, SSO and SSM.	The XXXX Action and Copy addressees receive the e-mail and attachment.		

## **ANNEX C     NATO AND NATIONAL CM PROCEDURES**

### **C.1   BI-SC CM PROCEDURE**

#### **C.1.1 CIS ORGANISATION AND MANAGEMENT**

A CIS Programme has to provide a new or upgraded operational capability to the users. It typically consists of the addition of new hardware and/or software to existing systems, or of the provision of new or upgraded systems. The scope of CIS is large and includes both the User Domain providing voice, telegraph, video teleconferencing, and core and functional area data services, as well as the underlying Network Domain including transmission, switching and security devices. Due to the evolutionary acquisition process of NATO CIS, a Programme is often divided in Increments. Each Increment is composed of one or several sub-system projects that are implemented almost together in time. The existing fielded systems that are part of the Programme are thus replaced/upgraded in different steps each time a new Increment is implemented.

Effective introduction of NATO CIS, especially when procured under an incremental programme, relies upon CM being an integral part of a sound life-cycle management structure that spans inception, implementation, in-service support, and disposal. In NATO the responsible authorities normally change during the stages of the life-cycle and hence the roles of the involved organisations and the relationships between them have to be clearly identified. A life-cycle management structure should, therefore, be established for all programmes at their inception. For NATO infrastructure programmes, the nomination of Authorities within the management structure as identified below will be included within the Capability Package. The required life-cycle management structure to be adopted for all programmes establishes a Programme Steering Group (PSG) and the three inter-related programme Authorities whose responsibilities are described below.

##### **C.1.1.1     Organisations**

- **Programme Steering Group (PSG).** The PSG involves representatives of the user, implementation and support communities. It shall be led by a representative of the principal user community. The PSG is responsible for the policy determination, guidance and direction of the programme, and hence has to remain continuously involved in all phases of procurement and in-service operation of all the concerned CIS that are part of the programme. The PSG is responsible for supervising the establishment of a programme CM structure. In the ACE environment, the PSG is the ACE ACCIS Steering Group chaired by the SHAPE CIS Assistant Chief of Staff (ACOS), with representation of the rest of the CM organisations (SMA, IMA and OSA), Senior users, Resource and Financial representatives, the ACE ACCIS Programme Management Office (PMO), etc.

- **System Management Authority (SMA).** The programme SMA is responsible for the major life-cycle planning and implementation scheduling activities of the CIS that are affected by the programme. This includes the management of operational deployment, infrastructure, and financial planning. The SMA is responsible for system coherence and interoperability throughout the programme life-cycle. The SMA may establish a Programme Management Office (PMO) to carry out its responsibilities on a day to day basis. For small programmes, the SMA may also undertake the role of the Steering Group. The SMA is responsible for the overall CM of the affected CIS throughout its life-cycle and will exercise this role through an SMA CM Board<sup>15</sup> (CMB) established as part of the programme management structure. The SMA CMB will, given approval by the PSG, normally delegate CM responsibilities to CMBs in other management Authorities as established. In the ACE context, the SMA role is taken by the SHAPE CIS Division with support from the ACE ACCIS PMO.
- **Implementation Management Authority (IMA).** The programme IMA is responsible for prototyping, development, procurement management, test and integration of the CIS aspects of the programme. The IMA is responsible for the delivery of a coherent and interoperable system in accordance with programme requirements. The IMA is responsible for the CM of those aspects delegated to it by the SMA CMB. This authority shall be exercised through an IMA CMB established as part of the programme IMA structure. Since a major IMA activity consists in the management of procurement contracts, the IMA CMB will normally delegate appropriate CM responsibilities to the Host Nations (HN) responsible for the individual procurement contracts. In the ACE context, NC3A is the IMA.
- **Operational Support Authority (OSA).** The programme OSA is responsible for all administrative and technical support to maintain the fielded CIS resulting from programme implementation. The OSA is responsible for the CM of those aspects delegated to it by the SMA CMB. This authority shall be exercised through an OSA CMB established as part of the programme OSA structure. The OSA CMB will delegate CM responsibilities to lower level Configuration Control Boards (CCB) or Offices (CCO) as appropriate. The NACOSA acts as the OSA for the ACE context.

---

<sup>15</sup> The SMA CMB corresponds to the STANAG 4159 Ed 2 Joint Configuration Management Committee or JCMC

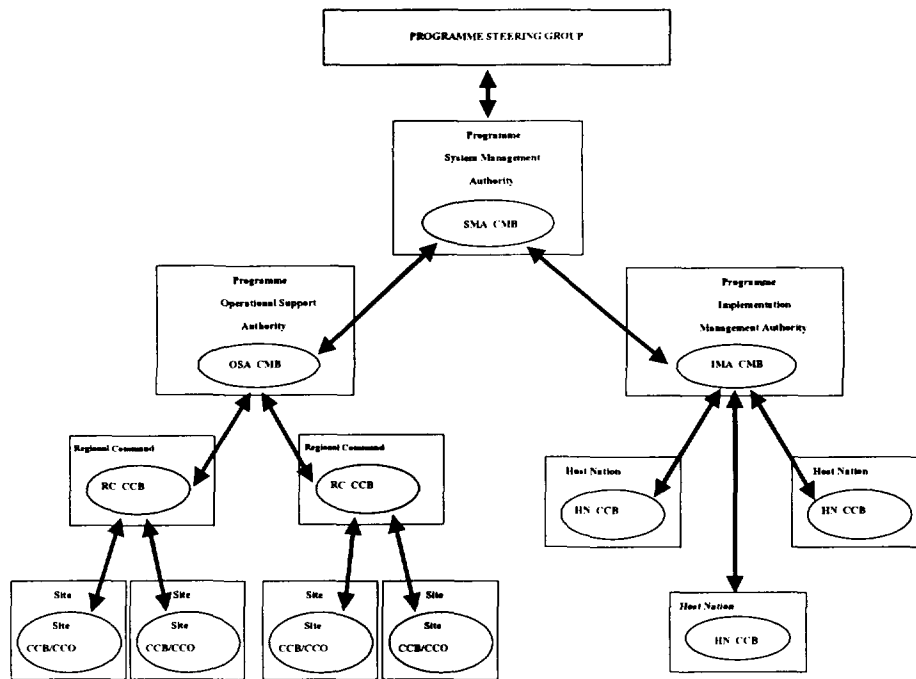


Figure C-1: Programme CM Management Structure

### C.1.2 Configuration Management Responsibilities

**NATO C3 Board:** The NC3B is the authority that establishes overall NC3 Organisation (NC3O) policy to ensure provision of cost effective, interoperable and secure NATO C3. It oversees the issue of general directives covering NATO CIS CM Policy and Guidance.

**NATO CIS Configuration Management Policy Group:** The NATO CIS Configuration Management Policy Group (CMPG) is responsible to the NC3B for:

- Developing, maintaining and promulgating NATO-wide CIS CM policy as required by the NC3B,
- Overseeing the implementation of, and compliance with, approved NATO CIS CM policy in respect of all NATO CIS,
- Providing guidance to resolve CM issues that lie beyond the authority of a single organisation,
- Within the context of Paragraph 1.6 of this Policy, monitoring interoperability issues within and between NATO and National programmes, and, where necessary, initiating action to resolve difficulties.

The CMPG will be responsible to the NC3B through AC/322(SC/5), the Information Systems Sub-Committee (ISSC). It will form a component of SC/5's sub-structure and will report as such. In fulfilling its role SC/5 will ensure all required co-ordination with other appropriate AC/322 elements.

**NATO Strategic Commands:** The SCs are responsible for ensuring compliance with the NC3B CIS CM Policy in their respective organisations, and for establishing the required management structure to support effective CM.

For programmes initiated by the SCs, the Commands are responsible for the establishment of PSGs and for nominating programme SMAs. For programmes that affect both SCs, a joint programme and CM structure with shared authority will be developed.

**NATO Consultation, Command and Control Agency (NC3A):** Given its central planning and systems integration role under the NC3O Charter, the NC3A will normally be identified as the programme IMA for NATO CIS Programmes. As such, the NC3A is responsible for establishing the required management structure to support effective CM during the implementation phase of the programme.

The NC3A will act as HN for individual projects when so appointed by the Infrastructure Committee.

The NC3A is responsible for ensuring compliance with the NC3B CIS CM Policy within its areas of responsibility.

The NC3A is also to provide vice chairmanship of and expertise to, the CMPG.

**NATO Communication and Information System Operating and Support Agency (NACOSA):** Given its NC3O Charter role for the operation and maintenance of the NATO C3 System (NC3S), NACOSA will normally be identified as the programme OSA for NATO CIS Programmes. As such, NACOSA is responsible for establishing the required management structure to support effective CM during the in-service phase of the programme.

NACOSA is responsible for ensuring compliance with the NC3B CIS CM Policy for the fielded systems assigned to it by the NC3B.

**NATO Maintenance and Supply Agency (NAMSA):** NAMSA is responsible for ensuring compliance with the NC3B CIS CM Policy for NATO CIS that are supported by NAMSA, and for providing technical and administrative CM support as further defined in the applicable Operating Instructions (OI).

**NATO ACCS Management Agency (NACMA):** Given its central planning and systems integration role under the NACMO Charter, NACMA will normally be identified as the programme IMA for ACCS programmes. As such NACMA is responsible for establishing the required management structures to support effective CM during the implementation phase of the programme.

NACMA will act as HN for individual projects when so appointed by the infrastructure Committee.

NACMA will be responsible for harmonising the requirements of the NACMO CM Policy for ACCS and the NC3B CIS CM Policy for the ACCS programmes within its area of responsibility.

**Host Nations:** Territorial HNs providing, implementing or maintaining NATO CIS are responsible for ensuring compliance with the NC3B CIS CM Policy within their respective



organisations in accordance with arrangements determined by the SMA, IMA or OSA as appropriate.

### **C.1.3 Configuration Management Process**

#### **C.1.3.1 General**

Configuration control is the management of a systematic change process exercised over the approved baselines of Configuration Items (CI). A configuration item is any piece or combination of hardware, software which is individually tracked and managed. The process provides:

- Before-the-fact analysis of change requirements so that the impact on interfaces, resources and schedules can be assessed.
- Formal approval of changes.
- A controlled implementation of the changes to both the physical system and its documentation so that system integrity can be maintained.

Configuration control begins once the first configuration document for a CI is approved and baselined which for a complete CIS system, will normally be the functional requirements as embodied in the approved functional baseline. The discipline must then be continued through to the final disposal of the CI, be it a complete system or a component.

Configuration Control involves the evaluation and disposition (including co-ordination and approval) of requests for changes to the Programme's Baselines. Decisions required for these tasks are made by CM Boards. Administrative support e.g. Configuration Control Offices to implement these decisions are provided by the SMA, IMA and OSA at the Programme Level.

#### **C.1.3.2 Configuration Change Proposal (CCP) Process**

Any change to the Fielded System or the System Configuration Data has to be initiated by raising a Configuration Change Proposal (CCP), which should be forwarded by the competent User Group to the appropriate CCB for approval. According to the delegated responsibilities, the decisions on CCPs will be taken as follows:

The top level CCB will decide on changes to the Fielded System with respect to:

- Changes to and distribution of centrally provided software.
- Update of the System Configuration Specifications
- Changes which will have an impact on the interoperability of the local Sub-Systems.

The Local CCB will decide on changes to the local Sub-System regarding:

- Changes to and implementation of site specific software, which has been or should be included in the Approved Fielded Product List.
- Changes to the hardware configuration according to the Minimum Hardware Specifications

The different level CMB/CCB may co-ordinate changes to the Fielded Sub-Systems within its area of responsibility. Upon major functional changes proposed by a User Group, the CCB may take the decision to realise the requirement through a new Capability Package (CP).

The top level CCB has to be informed about all decisions on changes to the Fielded Sub-Systems reached locally, in order to initiate dependent actions at central level (e.g. changes to the license requirements).

#### **C.1.4 Configuration Control Office (CCO) Processes**

##### **C.1.4.1 Central Co-ordination of Configuration Changes**

Upon decision of the top level CCB, the highest level CCO will co-ordinate all activities necessary to execute changes to the configuration of the Fielded System (Centrally provided Software). This process includes the Management of the Central CCPs (Registration, forwarding for further actions, monitoring and reporting on the status), as well as the Co-ordination of Central Software Releases (Initiation of new software versions, requesting required licenses), which includes the co-ordination of configuration changes with the local CCOs.

##### **C.1.4.2 Central Distribution of Software, Documentation, Media and Licenses**

Upon request the delivery of centrally provided CI will be prepared and executed. This includes the reproduction of required Media and the dispatch of the deliverables to the local CCOs. The CCO Data provides necessary information about the local CCOs (e.g. Mail addresses, POC).

##### **C.1.4.3 Central Control of Fielded System Data**

This process offers visibility to the Fielded System Baseline by providing baseline data required at the central level. For this purpose, the Central Fielded System Data (Accumulated/consolidated information about the local Sub-System Baselines, the CI structure) are maintained based on local Baseline data provided by local CCOs.

When necessary or decided by the top level CCB, local CCOs are requested to perform Configuration Status Accounting and Physical Configuration Audits to improve the quality of the Fielded System Baseline.

##### **C.1.4.4 Local Co-ordination of Configuration Changes**

Upon decision of the local CCB, the local CCO will co-ordinate all activities necessary to execute changes to the local software or hardware configuration of the Fielded Sub-System. This process includes required co-ordination with the highest level CCO (e.g. implementation date). The Local CCP Management will ensure proper registration of new CCPs and monitoring of their status. The Management of Software Implementation comprises site specific as well as centrally provided software. Finally, changes to the hardware configuration of the Fielded Sub-System have to be managed.

##### **C.1.4.5 Local Control of Fielded Sub-System Baseline**

The maintenance of the Fielded Sub-System Baseline is the major activity of this process. The CI and their attributes have to be documented and kept updated. The use of suitable inventory tools can support the collection of data about installed software and implemented hardware components. If requested or if necessary, Configuration Status Accounting and Physical Configuration Audits will be performed to improve the quality of the Fielded Sub-System Baseline.

#### **C.1.4.6 Local Distribution of Software, Media, Licenses, Documentation**

Upon receipt of centrally provided deliverables, or on request to implement site-specific software, these items are forwarded to the system administrator for installation. Received licenses have to be registered.

#### **C.1.5 Engineering Change Proposal (ECP) Process**

Changes to different types of product are market driven, with NATO control limited to determining if, when or how upgrades are to be implemented. The general approach is to use a specific “Strategic Products List” (SPL) – this list covers both hardware and software and is a matrix of services against products in Category 1 and services only for Categories 2 and 3.

Formal definitions are as follows:

**Strategic Products** are those products that have to be the same across NATO systems. The products have to be fundamentally the same to ensure that the integrity of the Core is assured.

##### **Category 1**

- Products that have to be the same across ACE and the product has been chosen due to the product being already in use.
- Essential for continued service or maintenance of investment

##### **Category 2**

- Products have to be the same across ACE but a product has not yet been chosen
- Required for providing new service
- Required for improving cost-effectiveness for existing service
- Required system-wide for specific purpose
- Choice of products available.

##### **Category 3**

- No specifically mandated product.
- Required for existing or new service
- Required in parts of the system
- Choice of products available

The NATO Open Systems Working Group (NOSWG) proposes a list of strategic products to the NC3B. NC3A develop the SPL from this. The Change Procedure for the SPL is given below.

- ECPs affecting the SPL may be submitted by User Groups, Commands (SC, subordinate) via the ACE change procedure or by the SMA, OSA, IMA, Host Nations, NATO HQ and ACE CCB
- The ECP shall be submitted to the IMA.
- The NATO standard form in ACMP-3 shall be used. Sufficient information to evaluate the ECP shall be provided even if the form can not entirely be completed.
- In urgent cases when all the information to support a formal ECP is not yet available, a preliminary ECP may be submitted. In this case only the first page of the ACMP-3 form is required supported by attachments if necessary.
- The submitter shall indicate the Class using the guidance below:

An ECP shall be Class 1 (Major) if:

- Integration into the site NS network of a new product (HW/SW) which is not mentioned in the SPL
- Important impacts e.g. cost, personnel, resources, effort for training/maintenance, functional impacts, change to standard, impact on interoperability

An ECP shall be Class 2 (minor) if it has no impact on the interoperability of the other products in the SPL or requires only minor resources:

- Software version update/upgrade e.g. (version 3.0 to 3.1)
- Change of hardware performance of workstation or servers e.g. (memory upgrade)
- The submitter shall clearly indicate the required change to the SPL.
- The submitter may indicate his number but the IMA will give a number in accordance with the ACE ECP numbering system.
- The submitter shall indicate the priority of the ECP:

Emergency ECP : An ECP which if not accomplished:

- May result in fatal or serious injury to personnel or in extensive damage or destruction of equipment
- May seriously compromise security

Urgent ECP : An ECP which, if not accomplished:

- May seriously compromise the mission effectiveness of deployed equipment or forces
- May seriously impact the functioning of the system
- Could result in injury to personnel or damage to the Equipment

- May cause significant contractual problems
- May cause significant life cycle costs if delayed

Routine ECP : All other ECPs.

- Treatment of Emergency ECP : The submitter takes every appropriate action to expedite implementation of the ECP. The submitter shall inform the IMA by the fastest possible means and forwards the ECP form as soon as possible. The IMA informs the IWG members, the AASG and others as required, as soon as possible. Target decision time **5 working days**.
- Treatment of Urgent ECPs : The submitter forwards the ECP form to the IMA who treats the ECP with the highest priority e.g. contact IWG members via E-mail etc. Target decision time **15 working days**.
- Treatment of Routine ECPs : The submitter forwards the ECP form to the IMA who treats the ECP during regular IWG meetings. Target decision time **45 working days**.

## **C.2 NETHERLANDS CM PROCEDURE FOR LAN2000**

### **C.2.1 LAN2000 release management strategy and organisation**

LAN2000 is a COE implementation of the MoD in the Netherlands. LAN2000 version 1 was designed in parallel with NC3TA version 1.0.

The products in the LAN2000 are divided into two bundles, the 'Basis Bundle' (BB) and the 'Additional Components' (AC).

The BB contains all essential functionality within the COE, e.g. operating system, E-mail, system management and office automation. The products in the BB have defence-wide been approved and standardized. Where LAN2000 is implemented, the products in the BB must be used to fulfil those functionalities that are already provided by products in the BB. In the NCOE model, the BB can be seen as those products implementing the common support application services and the required underlying infrastructure services and kernel services.

The AC are in fact the mission applications. Multiple products might be used to implement the same functionality. The update processes of the products in the AC are currently not centrally organised and are the responsibility of the functional owner of the product within the MoD.

Because most products in the BB are COTS, the lifecycle of the individual product must be monitored. The aim is to have full supported products in the BB. It is also desirable to implement terminal releases of the products, these releases are most stable and have the longest support. Based on the lifecycle of the individual products a LAN2000 release calendar is made on a yearly basis. BB releases are planned based upon this release calendar.

Within the LAN2000 concept the update process of the BB has four kinds of updates: small releases planned, small releases not planned, minor releases and major releases.

- Small releases planned are releases in a yearly-predefined release calendar. They contain releases per product and contain pro-active updates to guarantee the daily availability of the COE, e.g. monthly updates of anti-virus software. These releases have no or a small impact on the COE. Users of LAN2000 are not obligated to implement a small release.
- Small releases not planned are not planned in advance and contain fixes, like bug fixes or security hot fixes distributed by the manufacturer of the (COTS) software. These releases have no or a small impact on the COE. Small releases are releases per product. Depending on the nature of the release users or system management organizations will be strongly advised to install these releases.
- Minor releases have a minor impact on the COE and contain new functionality on products in the BB or new products replacing existing product with the same functionality. At minimum the minor release contains all publicized small (planned and not planned) releases, therefore, at a minimum, it is a baseline of the small releases. A minor release is scheduled and its content is announced in the release

calendar. Every year a minor release is planned and released in November. In figure C-2 the yearly update cycle of minor releases is shown.

### Lifecycle LAN2000 minor release

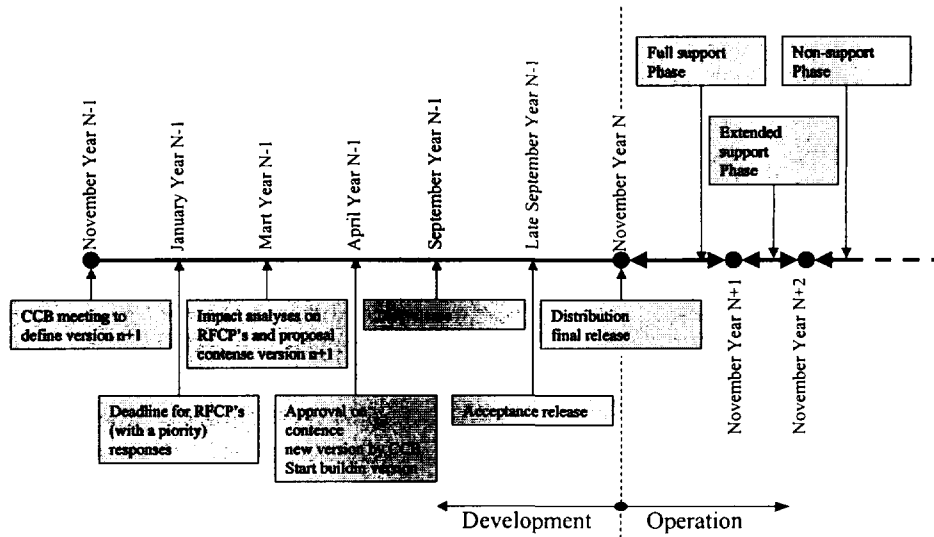


Figure C-2: Update Cycle minor releases

- Major releases contain changes in the architecture and therefore have a major impact on the COE (eg. a new version of the OS). A major release is planned well in advance but has no predetermined release cycle. Recently, a project has started to begin the development of a new major release.

All releases contain migration strategies. In principle changes in the LAN2000 BB are only proposed in areas where the new technology is gaining a broad market acceptance and mature product base.

LAN2000 has a Configuration Management Board (CMB), a Configuration Control Board (CCB) and a Software Control Board (SCB). In both the CMB and CCB, the information managers of the Chief of Defense and of all services represented. Also the LAN2000 development and support organization is represented at these boards.

All major changes must be approved by the CMB. Minor changes must be approved by the CCB. For each Request For Change Proposal (RFCP) an impact analysis is made to provide an overview on the risks, manageability, stability and impact on the other components of the COE. Also potential impact on the hardware must be provided.

The SCB is delegated to the LAN2000 development and support organization. After approval of the yearly release calendar of planned small releases by the CCB, the LAN2000 support organization starts to develop and deliver the small releases. The decision to release a small not-planned release is made by the LAN2000 support organization. Only the SCB knows in detail which version (release, service packs, fixes and patches) of the (COTS) products are implemented. The CCB only approves on product versions.

NOTE; In the NCOE the BOP contains only versions of products, therefore it is necessary before testing to get information on the actual version (service packs, fixes) that are operationally implemented. This information can only be given by the operational support organisation NACOSA.

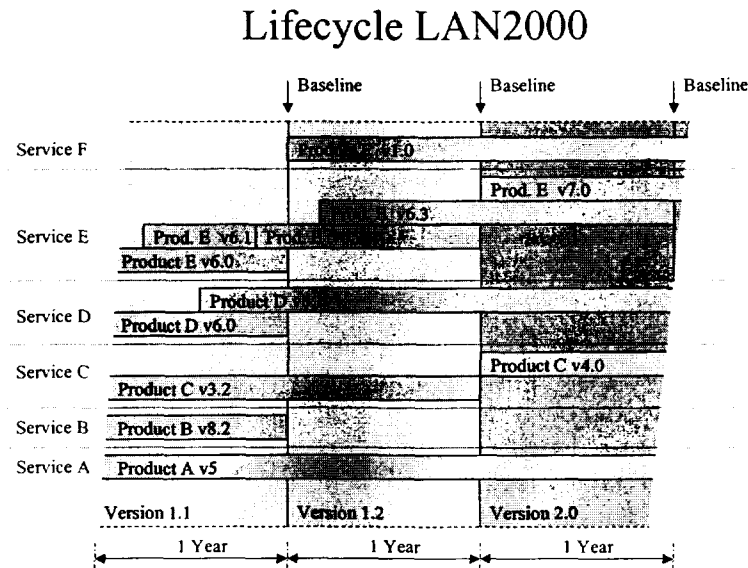


Figure C-3: Lifecycle LAN2000

In figure C-3 the LAN2000 lifecycle is illustrated. In figure C-4 on product E. As a user in principle is not obliged to implement a small release, two versions of the product must be supported. Product E v6.2 is a small release on Product E 6.1. When LAN2000 v1.2 (minor release) is released and implemented, Product E v6.0 is no longer supported.



Lifecycle LAN2000 version 1.1

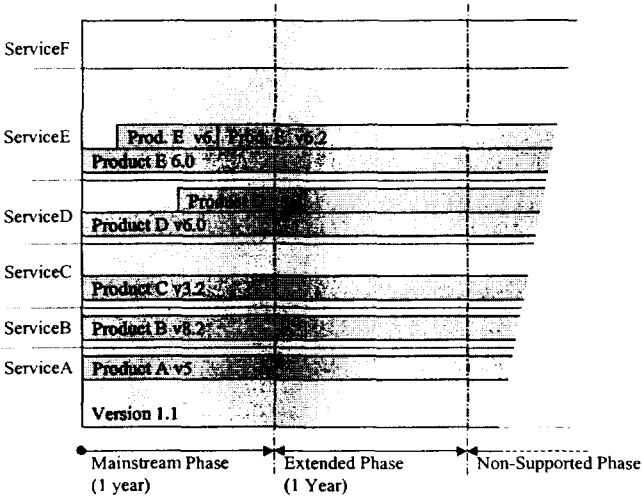


Figure C-4: Lifecycle LAN2000 version 1.1

A release has three support phases. In the first year (the mainstream phase) there is full support on the release. After this first year there is one year of extended support. After two years, the release is no longer supported.

## **ANNEX D    NC3TA TOOLS**

### **D.1 INTRODUCTION**

Many commercial tools are available on the market to support architectural development. There exist evaluation reports, both commercial (Gartner Group) and internal within NATO, that review the capabilities of these tools for specific architectural developments. The tool addressed in the section below has been developed specifically for the NC3TA and will become available through a NC3TA Web Portal as part of a broader guidance.

#### **D.1.1 Tool to support the selection or development process of interoperability profiles.**

In general, interoperability profiles consisting of a set of protocols and services in various layers and applications are quite complex. NC3TA includes supporting material and information through various volumes. Selecting or developing profiles, a project manager requires guidance and access to supporting information.

During the NCOE and IHP development process an GfIP (Guidelines for Interoperability Profiles) tool was designed in order to support project managers to select profiles or working groups responsible for the development of interoperability profiles.

The GfIP tool supports the profile selection and development process defined in the IHB. The primary goal is to provide easy access to the required information, distributed in diverse repositories. The availability of information facilitates the selection of a requested profile. In addition the GfIP tool will guide step-by-step through the defined development process (workflow) offering templates and examples for the definition of profiles.

The developed information package will be communicated to the responsible GfIP registration and maintenance authority, in order to revise the package and integrate it accordingly within the GfIP environment..

The tool includes links to

- the template for the definition of profiles - components and structure of interoperability profiles
- the selection /definition process for profiles - step-by-step web-based workflow
- the list and definition of already defined and existing profiles - profile information repository
- Supporting documentation, i.e. NCT3TA Volumes1-5, in particular sub-degrees of interoperability

- Glossary of terms

In addition, the development process is linked to a tool implementing a workflow for the development process. The result will be a complete set of information that is automatically enveloped in an email to the corresponding GfIP authority, requesting adoption and integration of the new developed profile within GfIP.

**Note:**

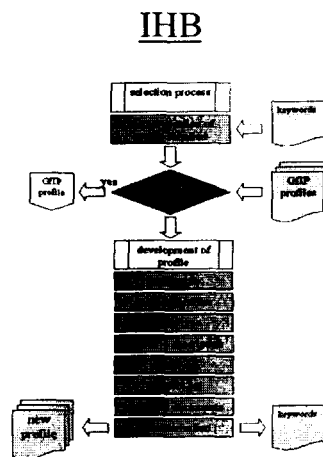
*The tool is valuable only if*

- *the concept of GfIP profile structure is adopted by NATO WGs responsible for the development of profiles,*
- *NATO WGs active develop interoperability profiles*
- *Somewhere takes the role of registration and maintenance authority*
- *requirements for the use of the GfIP are expressed by WGs*

The following page shows the starting Web page of the selection/development process .

## NATO C3 Technical Architecture

## Guidelines for Interoperability Profiles



Guidance for project managers or authorities responsible for the selection or development of interoperability profiles for interconnection of NATO/NATO and NATO/Nations domains

<u>Definition of Profiles</u>	<u>Selection/Definition Process</u>	<u>Profiles</u>	<u>Supporting Documentation</u>	<u>Glossary</u>
-------------------------------	-------------------------------------	-----------------	---------------------------------	-----------------

## **ANNEX E REFERENCES**

1. ***NATO C3 Technical Architecture (NC3TA), Allied Data Publication 34 (ADatP-34)***, dated 21 December 2001.
2. ***NIETI Concepts of Operations (CONOPS)***, AC/322(SC/2)N/150 dated 15 march 2001
3. ***NIETI Implementation Plan***, AC/322-WP/0154, dated 21 March 2001
4. ***Requirement for a Capability to support the C3 Interoperability Process***, AC/322(SC/2)L/56, 5 April 2001
5. ***Designed for Microsoft Windows NT and Windows 98 Logo Handbook for Software Applications***, Version 3.0d, 4 February 1999, Microsoft Corporation. This document provides details regarding the Design and conformance of applications for Windows NT and Windows 98;
6. ***Official Guidelines for User Interface Developers and Designers***, 2000, Microsoft Corporation. This document outlines the steps necessary to write applications with the same look and feel as Windows based applications.
7. ***NATO Security Committee and NC3B Primary Directive on INFOSEC***, AC/35-WP/240, AC/322-WP/0206.
8. ***NATO PKI Implementation Approach, architecture and assignment of responsibilities***, AC/322(NPMA)WP/07 Rev 2, dated 18 February 2002.
9. ***NATO Interoperability Management Plan (NIMP) Volume 2***, AC/322(SC/2)L(2002)/070, draft
10. ***NATO Architectural Framework, AC/322-D/0035, dated 10 November 2000.***

The Application Specifications information for MS Windows 2000 is available for downloading directly via <http://msdn.microsoft.com/certification/download.asp>.

Other relevant documents associated with the NC3TA may be accessed through each of the appropriate NATO web sites, or by contacting the secretary of the NOSWG, NHQC3S-ISTB, NATO HQ, and Brussels, Belgium. An electronic copy of the NC3TA may be accessed and/or downloaded at the following URL: <http://194.7.79.15>. The NIETI Core Team can be reached at: [NIETI@hq.nato.int](mailto:NIETI@hq.nato.int).